DENTONS

Privacy Review

Prepared for Oranga Tamariki
(Ministry for Children)

By Linda Clark

ORANGA TAMARIKI
Ministry for Children

Grow | Protect | Operate | Finance

April 2024 | Strictly confidential

Table of contents

Introduction

1 This review arose because of the Office of the Privacy Commissioner's (**OPC**'s) concerns about the handling of personal information by Oranga Tamariki. Since 2020, when it became compulsory for serious privacy breaches to be notified to the OPC, Oranga Tamariki has notified 35 breaches. These range from the unauthorised and mistaken release of an individual's name and address to the thoughtless disposal of a locked cabinet full of files of personal information. It is accepted that in more than one case the fact of the breach put lives at risk of actual physical harm.

2 Oranga Tamariki says of itself, 'we are dedicated to supporting any child in New Zealand whose wellbeing is at significant risk of harm now, or in the future. We also work with young people who may have offended, or are likely to offend'.[1]

3 Kaimahi can only carry out these roles – both in child welfare or youth justice – by collecting, holding, managing, sharing and publishing sensitive personal information about children, young people and their families, carers and associates.

4 This information is personal information as defined by the Privacy Act 2020 (**Privacy Act**).[2] It includes information about a child's birth, their health status, their mental health, where they are living and have lived, their schooling, their interactions with adults, details about trauma they have experienced and how they responded to it. It includes information about relatives and others which, if released, would identify the child or young person. Some of the information is factual, some of it is observational or opinion. In some cases the file held about an individual child runs to 10,000 pages or even longer. The file can span a whole lifetime, from birth to 25 years of age.[3] For some adults, who were previously children in care, this file is the only information they have about their own childhood and what happened to them. It is likely no other government agency holds so much sensitive information about individuals, nor retains it for so long.

5 Collecting this information and sharing it is crucial. Without it, kaimahi cannot make informed decisions about the welfare or placement of any child and unless the information is shared with others, adults cannot know enough to do what is best for each child or young person. Similarly, unless this information is released to former state wards they may never know their own story.

6 The core business of Oranga Tamariki is care and protection. Access to and use of personal information is an essential tool that allows kaimahi to protect children and young people but – more than that – the information collected and held about a child or young person is indivisible from the child or young person themselves. It is as precious as they are. Protect the information and you protect the child and vice versa.

[1] https://www.orangatamariki.govt.nz/

[2] Privacy Act 2020, s 7.

[3] Usually a young person leaves the care and supervision of Oranga Tamariki at age 18, but section 386AAA of the Oranga Tamariki Act 1989 allows for young persons up to the ages of 21 and 25 to be assisted in certain circumstances.

This review and its methodology

7 This review was commissioned to assist the senior leaders of Oranga Tamariki understand the reasons why privacy breaches continue to happen, to identify any patterns in the breaches (if they exist) and to improve the way kaimahi collect, manage, use and retain personal information.

8 The review's Terms of Reference require the reviewer to focus on:

a the policies, practice guidelines and training materials that define and describe how kaimahi should collect, manage, use and retain personal information;

b the way kaimahi apply these policies, practice guidelines and training in the field and in their interactions with each other, their clients and other agencies with which they interact in the course of any working day;

c the systems in place to manage and retain personal information and how kaimahi use these systems in the way they carry out their roles on any working day;

d identifying patterns, if such patterns exist, between previously notified privacy breaches. This could include patterns demonstrating the kinds of behaviours that lead to breaches, the kinds of roles in which kaimahi most commonly breach the Privacy Act and / or offices or parts of Oranga Tamariki where breaches have commonly occurred; and

e the way Oranga Tamariki has responded to previous privacy breaches.

9 The review was not intended to be an investigation of any particular privacy breach, nor to result in any individual or individuals being blamed for any particular breach. Rather, the review is intended to assist senior leaders at Oranga Tamariki better understand the privacy culture of the organisation and to identify what, if any, steps might reduce the likelihood of future privacy breaches.

10 To complete this report:

a we reviewed:

i all relevant policies currently in place;

ii all relevant training modules;

iii the various technology systems used by kaimahi;

iv information about privacy breaches notified to the OPC;

b we interviewed a range of employees across all levels of the organisation, and from different locations, including kaimahi working in child welfare and youth justice residences; and

c we met with the Deputy Privacy Commissioner and other OPC kaimahi who have previously investigated privacy breaches at Oranga Tamariki.

11 Prior to finalising this report, we also provided a draft version for comment to the Privacy Officer and the Deputy Chief Executive responsible for People, Culture & Enabling Services at Oranga Tamariki. Feedback from them was incorporated into the final report.

12 We acknowledge the cooperation of all Oranga Tamariki kaimahi who were approached during the preparation of this report and who assisted us by providing information and / or constructive observations and reflections. They were open, frank and above all committed to the children and young people they are employed to protect. While this report contains criticism of the privacy culture and processes of Oranga Tamariki, it is not intended to be a criticism of any of the people who work there. They do important work, often thanklessly and in challenging circumstances.

Summary

13 The core business of Oranga Tamariki is the care and protection of children and young people. To do this it must also care for and protect the personal information of children and young people. The simple fact is a child and their personal information is indivisible. Yet this appears to be little understood by kaimahi at the agency.

14 Oranga Tamariki has experienced a high number of notifiable privacy breaches since December 2020 when privacy laws changed and it became compulsory for serious privacy breaches to be reported to the Privacy Commissioner. It is not possible to say how many other breaches have occurred during this time because record keeping is not reliable and kaimahi spoken to for this review admitted not all breaches (i.e. those that would not meet the legal threshold for notification) are reported.

> *I have too many things on my plate to think about privacy when it's not in my portfolio at the moment.*

15 Overall, we found the privacy culture to be one of low maturity. There are skilled and motivated individuals working on improving compliance with the Privacy Act, but their best efforts alone will not shift the dial. A fundamental cultural shift, led from the top, is required if privacy considerations are to be incorporated into the everyday tasks kaimahi already do and further privacy breaches are to be prevented. First, though, there are significant roadblocks to overcome, including but not limited to the following.

Privacy is simply not top of mind

16 Most Oranga Tamariki kaimahi have become used to not thinking about privacy considerations. If they do think about privacy, they perceive it as an extra complication and something on top of their 'business as usual' care and protection obligations to children and young people. Many staff we spoke to described themselves as too busy to think about privacy.

Access to information is not sufficiently protected

17 Oranga Tamariki operates a high trust, high risk information management system. It holds extraordinarily large amounts of personal information about thousands of vulnerable children and their families. This information is held on a number of different computer systems. The largest of these systems is CYRAS, to which the majority of Oranga Tamariki staff have access.

18 We were surprised to learn only 0.6% of the information held by Oranga Tamariki is considered sensitive enough to have restricted access. In practice, too many staff have access to more information than they need to carry out their work.

Not all breaches are reported

19 There is evidence serious breaches (breaches with the potential to cause serious harm) are identified and reported. Oranga Tamariki staff appear to understand their obligations under section 114 of the Privacy Act to notify the Privacy Commissioner of any notifiable breach.

20 But it appears to be less well understood that *any* breach of any of the Information Privacy Principles (**IPPs**) set out in section 22 of the Privacy Act may lead to an interference with the privacy of an individual.[4] Also, not well understood is the fact that a breach is not only the unauthorised sharing of personal information with a third party. Breaches can be a range of acts or omissions including talking about a child with a co-worker who has no legitimate reason to know or leaving a document on a desk so others can read it or failing to delete notes about a child that were recorded on a personal phone.

[4] Privacy Act 2020, s 69(2)(a)(i).

Workplace practices are inconsistent with good privacy culture

21 The review was told of a range of workplace practices that are high risk and give rise to opportunities for the misuse of personal information. There is no evidence this is deliberate. But where kaimahi effectively quarantine privacy considerations as something different to and less than the care and protection of children then this will be reflected in the way they work.

Prevention needs to come first

22 The agency has an effective response plan for when serious breaches occur. It recognises that, because of the sensitive nature of the personal information held and the vulnerable circumstances confronting many affected families, speedy action is necessary in some cases where the subsequent risk of physical danger is real.

23 But we did not see evidence initiatives to prevent breaches occurring in the first place extends beyond basic online training held once a year, some refresher sessions at certain sites, and online resources to promote privacy week. While the agency has a relatively high compliance rate with its training modules, the anecdotal evidence (and the repeated breaches) suggests this is not enough.

Privacy is not seen as everyone's responsibility

24 Kaimahi often consider privacy to be someone else's job. There are individuals within the business whose roles are specifically targeted at privacy education and / or management but they are not responsible for ensuring all personal information is properly collected, used and disclosed. Every person at Oranga Tamariki who collects, reads, considers or shares information about children and young people is responsible for keeping that personal information safe.

Policies alone won't fix this

25 Oranga Tamariki has extensive policies but there are too many of them and they are not presented in an accessible way.

Technology alone won't fix this

26 The computer and information management systems of Oranga Tamariki are often criticised by kaimahi as being slow, cumbersome and getting in the way of safe privacy practices.

27 At the same time, kaimahi still commonly rely on paper and some reported not using digital communications services such as the agency's intranet, Te Pae (which contains all privacy policies and where privacy related announcements are posted).

28 Oranga Tamariki has a programme underway to update and improve its information systems. But this alone will not improve either the culture or compliance with privacy measures.

There is insufficient monitoring and accountability

29 Oranga Tamariki does not proactively monitor the way its kaimahi access and use personal information. It does respond whenever a concern about usage is raised, including sometimes conducting 'footprint' analysis to check who has accessed a file and why. But without a regime of active monitoring it cannot reassure itself that individuals are not misusing the privileged access they have.

30 The agency's preference is to educate, rather than enforce. There are two issues with this approach. Firstly, the general lack of awareness about what privacy means and how integral it is to the core business of Oranga Tamariki demonstrates that education alone is not working. Secondly, accountability processes and enforcement naturally sit alongside and support education. This is not a case of either or; both will be required if the privacy culture of Oranga Tamariki is to be improved and matured.

Leadership matters

31 It was difficult to ascertain who in Oranga Tamariki leads the agency’s overall privacy approach. Instead we found a range of capable people working in different parts of Oranga Tamariki, often with a narrow remit. There were no clear lines of accountability or ownership. Yet effective leadership will be needed if Oranga Tamariki is to make the scale of cultural shift required to improve its privacy culture and reduce the likelihood of future privacy breaches.

32 We heard from a number of kaimahi who reported a reluctance to change their workplace practices, either because they wanted to avoid putting more stress and expectation on busy social workers or because they were comfortable with working a certain way. This presents a challenge which only good leadership can overcome.

Next steps – recommendations

33 The changes required to improve privacy management and compliance at Oranga Tamariki rely on a values reset, changes in workplace practices and expectations and leadership. Taken together they represent a significant culture shift.

The values reset

34 The pou that supports (or ought to support) the work at Oranga Tamariki is the Oranga Tamariki Act 1989 (**Oranga Tamariki Act**) and in particular two key provisions, namely that:

a the well-being and best interests of the child or young person are the first and paramount consideration;[5] and

b the well-being of a child or young person must be at the centre of all decisions affecting that child or young person.[6]

35 In all respects these statutory requirements are entirely consistent with the Privacy Act and the IPPs contained in it.[7]

36 In fact, if the Oranga Tamariki Act can be considered a pou, then the Privacy Act is its natural companion. The two statutes require Oranga Tamariki to keep children and young people safe, since the child is indivisible from their personal information.

37 Oranga Tamariki kaimahi should be encouraged to see their obligations under both statutes as being complimentary and aligned. They cannot give paramountcy to the interests of the child under the Oranga Tamariki Act if they ignore their obligations to protect the personal information of the child under the Privacy Act.

38 Any person who has access to the personal information of another must understand the obligations that imposes. Personal information needs to be handled with the greatest of care. Kaimahi understand, or ought to understand, their special duties concerning the welfare and safety of the many vulnerable children and young people with whom they work. They also need to understand that information about these children and young people requires the same level of sensitivity and diligence. It is no exaggeration to say that lives can depend on it.

Changes in workplace practice

39 Kaimahi who are not thinking about privacy do not fully understand what privacy is and how it is infused in everything they do. They could not do their jobs without access to personal information. To shift thinking, an agency wide education programme is required to upskill all kaimahi on what the Privacy Act means, how to incorporate it into their daily tasks and how complying with the Privacy Act will help to keep children and young people safe.

40 This will require, as a first step, updating policies to ensure that they are compact, accessible and fit for purpose.

41 Oranga Tamariki should also consider replacing the current online teaching tool with more intensive training, preferably face to face and with training exercises based more closely on lifelike scenarios. Any individuals who are found to be breaching privacy policies should be required to complete refresher courses. In addition, the following practical steps can be taken:

a There is no need for Oranga Tamariki kaimahi to have unrestricted access to all information about all children and young people in the agency's care. Case files should be categorised to limit access to only those who need to know, and access to information in each file should be

[5] Oranga Tamariki Act 1989, s 4A.
[6] Oranga Tamariki Act 1989, s 5(1)(b).
[7] Privacy Act 2020, s 22.

gated to minimise access appropriately. These protections can be supported by good processes for seeking additional approvals to access information if and when circumstances change.

b As part of the cultural shift required at Oranga Tamariki, workplace practices need to be reviewed to ensure that personal information is not shared inadvertently with co-workers and outside parties. Clear guidance is needed on practical ways to manage documents, share information in group settings and maintain confidentiality. This may require upskilling some kaimahi in basic computer skills and encouraging all staff to use digital records in preference to paper.

Increased accountability and performance tracking

42 The upskilling of staff needs to be accompanied by the introduction of transparent and effective accountability measures. All kaimahi need to know who is responsible for the overall privacy programme, where to turn for help on a privacy question, how to report a near miss or breach, and what will happen if they do. Monitoring and reporting processes are key tools to both encourage compliance and to track it. To this end, we recommend:

a The introduction of transparent privacy targets.

b Quarterly reporting to the Chief Executive and senior leadership team of a range of identifiable outcomes. These could include the number of notified breaches, the number of other breaches, the number of reported near misses, the number of privacy complaints registered with Oranga Tamariki, the time taken to respond to a request made under the Privacy Act for personal information, reports on random checks for employee browsing and spot site visits to check on document and information management. The objective of this reporting is to drive a prevention first approach.

c Centralisation of the privacy roles across the organisation to better align delivery and performance.

d Elevation of the Privacy Officer role to signal to all kaimahi the importance of privacy and compliance with the Privacy Act.

43 A table of recommended actions is included at the end of this report.

44 Lastly, one common theme that emerged from the interviews with kaimahi was the observation that Oranga Tamariki is good at starting new projects, but very poor at completing them. To avoid that happening here, we recommend a review be undertaken in 12 months’ time to provide senior leaders with reassurance about progress against the recommended action points.

45 The notified breaches that prompted this review have, in some cases, already put individuals in physical danger. Further breaches could do the same and worse.

46 We recommend sharing this report with the OPC and the Children’s Monitor. Both have an interest in ensuring Oranga Tamariki makes progress.

Oranga Tamariki – legislative and regulatory framework

Overview

47 The information Oranga Tamariki holds is precious. It is highly sensitive in nature and involves children, young people and their whānau. It is reasonable for the public to expect Oranga Tamariki to treat the information it holds with respect and care, recognising both the inherent value in privacy and the fact that Oranga Tamariki has a legal duty to ensure that its collection, use, holding and disclosure of personal information is lawful.

48 Failure to comply with privacy law not only has legal consequences, but fundamentally impacts public trust. Compliance with privacy law therefore allows Oranga Tamariki to fulfil its role as kaitiaki of personal information which in turn gives Oranga Tamariki the social licence to function effectively.

49 This part sets out the applicable legislative and regulatory context within which Oranga Tamariki operates.

50 By way of summary:

a Oranga Tamariki was established under the Act now known as the Oranga Tamariki Act. Among other things, the Oranga Tamariki Act authorises information sharing between authorised child welfare and protection agencies and authorised independent persons. The personal information relating to a child or young person, irrespective of the purpose for which that information was collected, may be used or disclosed for a number of specified purposes, one of which is to prevent or reduce the risk of a child or young person being subject to harm, ill-treatment, abuse, neglect, or deprivation.

b Oranga Tamariki is subject to the IPPs under the Privacy Act, which govern the collection, use, retention, and disclosure of personal information. The Health Information Privacy Code 2020 (**HIP Code**) establishes health information privacy rules (**HIP Rules**), which modify the IPPs in respect of ‘health information’ and which arguably apply to Oranga Tamariki in the context of Oranga Tamariki arranging for the delivery of health services to children and young persons, and otherwise in the context of its handling of health information. Among other obligations, Oranga Tamariki is required to protect the personal information (including health information) that it holds against misuse, and only use that information for the purposes for which Oranga Tamariki collected it for.

c Oranga Tamariki is also subject to the Family Violence Act 2018 (**FVA**). Among other things, the FVA authorises Oranga Tamariki to make information requests, use, and disclose personal information about a victim or perpetrator of family violence from any family violence agency or social services practitioner, for a number of purposes, one of which is to help ensure that a victim is protected from family violence.

51 For completeness:

a Oranga Tamariki, like other Crown entities, is subject to the Official Information Act 1982 (**OIA**) which allows individuals and New Zealand companies to request the disclosure of ‘official information’ held by Oranga Tamariki. Subject to limited exceptions, Oranga Tamariki must provide the information requested.

b Oranga Tamariki has further information management obligations under the Public Records Act 2005 (**Public Records Act**), and the Information and Records Management Standard issued under the Public Records Act. Among other obligations, Oranga Tamariki must ensure that information is managed and retained appropriately and that information is protected from unauthorised or unlawful access, alteration, loss, deletion, and destruction. These information management obligations are supplemented by additional obligations under the Oranga Tamariki

Act (and associated regulations) which specifically require Oranga Tamariki to maintain records regarding children and young persons within its care.[8]

c As a Crown entity, Oranga Tamariki is also subject to the Public Service Act 2020 which describes the principles (the fundamental features of the way in which the public service operates) and values (the necessary behaviours of public servants to maintain the integrity of the public service) underpinning New Zealand's public service.

52 Oranga Tamariki (as an organisation) and kaimahi (as agents of the organisation) are subject to the obligations each of the statutes, standards and codes impose on them.

Privacy Act

53 Privacy law in New Zealand is primarily governed by the Privacy Act. The IPPs are the pillars of the Privacy Act, as these regulate how Oranga Tamariki collects, holds, uses and discloses personal information. The Privacy Act also provides for rights of individuals in respect of their personal information, and prescribes the actions that an agency must take following a privacy breach.

54 The concept of personal information under the Privacy Act is broad and defined as any information about an identifiable individual.[9] This definition means that information may be personal information and therefore captured by the Privacy Act if there is some 'link' in the information which means the individual is able to be identified. One such example is an address. Even if an individual is not explicitly named, that address may still be used to identify who lives at that location, and so is captured by the definition of personal information.

Health information

55 The HIP Code, established by the Privacy Commissioner pursuant to the Privacy Act, provides the HIPC Rules, which modify the IPPs in respect of health information that is collected, held, used, and disclosed by 'health agencies'. While it is arguable that the HIP Code does not apply to Oranga Tamariki directly (since Oranga Tamariki does not itself provide 'health services'), there is such a close nexus between Oranga Tamariki and the services that it arranges for the benefit of children and young persons, which involves the handling of sensitive health information about those children and young persons, that it would seem incongruous to not hold Oranga Tamariki to the same higher standard under the HIP Code than would apply to other agencies involved in the provision of health services who deal routinely with health information..

56 Accordingly, the higher standard of care required by the HIPC Rules arguably applies to health information held by Oranga Tamariki, rather than the IPPs. Health information includes the following classes of information: [10]

a information about the health of an individual, including their medical history;

b information about any disabilities an individual has, or has had;

c information about any health services or disability services that are being provided, or have been provided, to an individual; and

d information about an individual, which is collected before or in the course of, and incidental to, the provision of any health service or disability service to that individual.

[8] For example, regulation 70 of the Oranga Tamariki (National Care Standards and Related Matters) Regulations 2018 requires the Chief Executive of Oranga Tamariki to ensure that, in relation to a child or young person in care or custody, ensure that a record of important events, achievements, relationships, and other matters in the child's or young person's life (for example, photos, art work, and school reports) is collected, recorded, and maintained.

[9] Privacy Act 2020, section 7.

[10] Health Information Privacy Code 2020, r 4.

Application of Privacy Act and HIPC Rules to Oranga Tamariki

57 In the context of the use of and access to information within Oranga Tamariki:

a the HIPC Rules apply to the use, storage, and disclosure of health information by Oranga Tamariki; and

b the Privacy Act otherwise applies to the use, storage and disclosure of personal information by Oranga Tamariki.

58 The Privacy Act and HIPC Rules are intended to establish an underlying framework, which informs (but does not negate) legislative provisions that govern the holding, use, disclosure, and processing of personal information. The Privacy Act and the HIPC Rules do not override or limit any other provision contained in a New Zealand statute that authorises or requires personal information to be made available, or otherwise regulates the way personal information is obtained.[11] This means that it is not a breach of privacy law to disclose, use or collect information if that action is authorised or required under another law.

59 For Oranga Tamariki, this means that its obligations under the Privacy Act should be viewed in the context of the Oranga Tamariki Act, including its duty to promote the well-being of children, young persons, and their families, whānau, hapū, iwi and family groups.

Oranga Tamariki Act

60 The overarching purpose of the Oranga Tamariki Act is to 'promote the well-being of children, young persons, and their families, whānau, hapū, iwi and family groups' through numerous means.[12] This is underpinned by the 'paramountcy principle' which means the 'well-being and best interests of the child or young person are the first and paramount consideration'.[13]

61 The framework for information sharing is primarily established by sections 66-66Q of the Oranga Tamariki Act. The purpose of these sections is to facilitate the gathering and sharing of information to achieve the purposes of the Oranga Tamariki Act, and that persons carrying out functions under the information sharing clauses must have regard to the paramountcy principle which takes precedence over any duty of confidentiality owed by Oranga Tamariki in relation to the child or young person, or any person who is a family member of that child or young person or in a family relationship with that child or young person (within the meaning of section 12 of the FVA).[14]

62 The framework for information sharing prescribes the purposes for which a child or young person's personal information may be used under the Oranga Tamariki Act, irrespective of the purpose for which the information was collected. The Oranga Tamariki Act authorises the use of information for the purposes of:[15]

a preventing or reducing the risk of a child or young person being subject to harm, ill-treatment, abuse, neglect, or deprivation;

b making or contributing to an assessment of risk or need in relation to a child or young person, or any class of children or young persons;

c making, contributing to, or monitoring any support plan for a child or young person, where the plan relates to the activities and functions of Oranga Tamariki;

[11] Privacy Act 2020, s 24.
[12] Oranga Tamariki Act 1989, s 4.
[13] Oranga Tamariki Act 1989, s 4A.
[14] Oranga Tamariki Act 1989, s 65A.
[15] Oranga Tamariki Act 1989, s 66C.

d preparing, implementing, or reviewing any prevention plan or strategy issued by Oranga Tamariki;

e arranging, providing, or reviewing services facilitated by Oranga Tamariki for a child or young person and their family or whānau; or

f carrying out any function in relation to family group conferences, children or young persons in care, or other functions relating to care or protection.

63 Disclosure of personal information is also authorised if that disclosure is to another child welfare and protection agency or an independent person if Oranga Tamariki reasonably believes that disclosing the information will assist the agency or independent person receiving the information to carry out any of the purposes described directly above.[16]

64 Similarly, the Oranga Tamariki Act authorises the disclosure of information for the purposes set out at paragraph 62(a) – (f) above.[17]

65 Sections 66L to 66Q of the Oranga Tamariki Act contemplate the establishment and approval (by the responsible Minister) of a Code of Practice for Information Sharing (**Oranga Tamariki Code**).[18] The purpose of the Oranga Tamariki Code is to provide both guidance and direction to child welfare and protection agencies and independent persons about the application of the information sharing provisions of the Oranga Tamariki Act and how disputes about the interpretation and application of those provisions should be resolved.

Interaction with Privacy Act

66 If there is any inconsistency between the information sharing provisions in the Oranga Tamariki Act and the Privacy Act, the Oranga Tamariki Act provisions are to prevail.[19]

67 While many Oranga Tamariki kaimahi we spoke to understood the fact that Oranga Tamariki has obligations under both the Privacy Act and the Oranga Tamariki Act, a common theme was confusion about how these two statutes worked together in practice. It is important from the outset to clarify that there is no tension between the Privacy Act and the Oranga Tamariki Act. Information use and disclosure that is permitted under the Oranga Tamariki Act is authorised under the Privacy Act.

68 One way of conceptualising this is the notion that the Oranga Tamariki Act is a singular pou. It supports and guides kaimahi to do their job and permits personal information to be used and disclosed for specific purposes (primarily, to keep children and young people safe). The Privacy Act is an equal pou that also exists to assist kaimahi to do their job and keep children and young people safe. The Privacy Act does not create any additional burden or a push / pull dynamic with the Oranga Tamariki Act.

69 This is not to say that Oranga Tamariki employees – particularly frontline kaimahi – have an easy task in knowing when to use or disclose information and when to withhold. A fundamental understanding of children and young people and their whānau's circumstances is needed to be confident in knowing when information may or may not be lawfully used or disclosed in accordance with the Oranga Tamariki Act and the Privacy Act.

70 However, the information sharing provisions of the Oranga Tamariki Act allow for kaimahi to deal with those 'grey area' situations in a more confident way. While the Privacy Act authorises the disclosure of information for a number of reasons (including that the use of the information is

[16] Oranga Tamariki Act 1989, s 66C(a).

[17] Oranga Tamariki Act 1989, s 66C(b).

[18] Guidance for sharing information across the child welfare and protection sector is available at https://www.orangatamariki.govt.nz/assets/Uploads/Working-with-children/Information-sharing/Information-sharing-Guidance-OT-Act-1989.pdf. It is not clear to us that this guidance is the 'Code' contemplated by sections 66L to 66Q of the Oranga Tamariki Act (since it does not appear to have been formally approved in the manner contemplated by the Act). The Code, if properly approved in accordance with the Oranga Tamariki Act, would be secondary legislation.

[19] Oranga Tamariki Act 1989, s 66Q.

necessary to prevent or lessen a serious threat to the life or health of the individual), the Oranga Tamariki Act clarifies that the interests of the child are paramount. Any use or disclosure of information that is permitted under the Oranga Tamariki Act will therefore not constitute a breach of the Privacy Act.

Specific obligations when dealing with personal information

71 Set out below are the specific obligations Oranga Tamariki has under the Privacy Act and Oranga Tamariki Act when dealing with personal information.

Collection of information

72 Under IPP 1 of the Privacy Act, Oranga Tamariki **must only collect personal information for a lawful purpose**, connected with a function or activity of Oranga Tamariki business (and then only so much information as is necessary for that lawful purpose). The Oranga Tamariki Act prescribes that any individual or New Zealand company must, upon request, supply to Oranga Tamariki any information held by them that may relate to or affect the safety or well-being of a child or young person, if that information is required to determine whether a child or young person is in need of care or protection or assistance or for any proceedings under the Oranga Tamariki Act (including a family group conference).[20]

73 IPP 2 prescribes that Oranga Tamariki **must only collect personal information directly from the individual concerned** (unless Oranga Tamariki reasonably believes that compliance would prejudice the purposes of collection or another exception applies). The nature of the statutory function of Oranga Tamariki means that a significant portion of client information obtained by Oranga Tamariki is obtained from third parties (such as other government agencies, schools, medical professionals, other whānau and family members) in reliance on the information-gathering powers under the Oranga Tamariki Act, such that Oranga Tamariki is not required to comply with IPP 2. In other circumstances where Oranga Tamariki does not collect information directly from the relevant individual, Oranga Tamariki may be able to establish that such collection is permitted under the exemptions to IPP 2 or HIPC Rule 2 (as the case may be).[21]

74 IPP 3 states that when collecting personal information directly from individuals, Oranga Tamariki **must take all 'reasonable steps' to ensure that clients are aware of** (among other matters) **the fact and purposes for which their personal information may be held** and used by Oranga Tamariki. This means taking care to make sure clients understand the way information is used within Oranga Tamariki, including how information may be accessed and used internally. There may regularly be circumstances where the wellbeing of a child or young person and/or the circumstances in which information is collected will trump the requirements of IPP 3, and an IPP 3 exception will apply (such as compliance is not reasonably practicable in the circumstances of the particular case, or will prejudice the purposes of collection).

75 Under IPP 4, Oranga Tamariki **must only collect personal information by a means that is lawful** and, in the circumstances, fair and not unreasonably intrusive – particularly in circumstances where personal information is being collected from children or young persons.

Storage and security of information

76 In accordance with IPP 5, Oranga Tamariki **must ensure that the personal information it holds is protected** by such security safeguards as are reasonable in the circumstances to take against:

a loss;

b access, use, modification, or disclosure not authorised by Oranga Tamariki; and

[20] Oranga Tamariki Act 1989, s 66.
[21] Oranga Tamariki Act 1989, s 66Q.

c other misuse.

77 Documents containing health information to which the HIP Code applies must also be disposed of in a manner that preserves the privacy of the individual concerned.

78 The nature of the information that Oranga Tamariki holds is such that the security safeguards in place to protect client information must meet a higher standard than those applied to information of a less sensitive nature. This involves both technical safeguards and organisational measures to prevent not only inadvertent disclosures of personal information, but also to mitigate the risk of unauthorised access to information within Oranga Tamariki.

Access to and correction of personal information

79 Under IPP 6, **an individual is entitled to receive access to any personal information that Oranga Tamariki holds about them**. An individual is also entitled to request the correction of that information under IPP 7.

80 An additional requirement under IPP 7 is that Oranga Tamariki must take steps that are reasonable in the circumstances to ensure that, having regard to the purposes for which the information may lawfully be used, **the information it holds is accurate, up to date, complete, and not misleading**. Under IPP 8, Oranga Tamariki must not use or disclose any personal information without taking any steps that are, in the circumstances, reasonable to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

Retention of information

81 IPP 9 requires that Oranga Tamariki **must only keep personal information** (including health information) **for as long as is required** for the purposes for which that information may lawfully be used. This obligation is subject to any statutory minimum retention periods, including retention periods contemplated by the Public Records Act, the Oranga Tamariki Act itself, and regulations made under the Oranga Tamariki Act. On 28 March 2019, the Chief Archivist issued a general notice revoking authority to dispose of any records which may be relevant to the Royal Commission into Abuse in Care.[22] We understand that Oranga Tamariki has interpreted this broadly. This has effectively prevented Oranga Tamariki from disposing of much of the information relating to its core functions.

82 Under the HIP Code, Oranga Tamariki is permitted to keep any document containing health information, the retention of which is necessary or desirable for the purposes of providing health services to the individual concerned.[23]

83 In the case of health information to which the Health (Retention of Health Information) Regulations 1996 applies (which, similar to the HIP Code, arguably applies to Oranga Tamariki on the same grounds), the minimum retention period is 10 years beginning on the day after the date shown in the health information as the most recent date on which a provider provided services to that individual.[24]

Limits on use and disclosure of information

84 IPPs 10 and 11 regulate the use and disclosure of information. This means that, unless otherwise permitted by another enactment, (including the Oranga Tamariki Act), Oranga Tamariki **may only use and disclose personal information** (including health information) that Oranga Tamariki holds:

a **for the purposes for which Oranga Tamariki obtained that information**;

[22] Archives New Zealand *General Notice Revoking Authority to Dispose of Public Records relevant to the Royal Commission of Inquiry into Historical Abuse in State Care and in the Care of Faith-based Institutions* (28 March 2019).
[23] Health Information Privacy Code 2020, r 9.
[24] Health (Retention of Health Information) Regulations 1996, reg 6.

b for directly related purposes; or

c for one of the other limited grounds of use provided by HIPC Rule 10 (in the case of health information) or by IPP 10 (in the case of all other personal information).

85 In the context of IPP 10, Oranga Tamariki will be considered to have 'used' information when processing that information within Oranga Tamariki, including when information is shared between kaimahi. This means that Oranga Tamariki must be able to point to a lawful purpose whenever a staff member accesses a client file (as well as when using information within a client file).

86 Oranga Tamariki may, irrespective of the purpose for which information relating to a child or young person or any class of children or young persons was collected:[25]

a use that information for a number of purposes, such as preventing or reducing the risk of a child or young person being subject to harm, ill-treatment, abuse, neglect, or deprivation; or

b disclose (whether on request or on the agency's or independent person's own initiative) that information to another child welfare and protection agency or an independent person if the agency or independent person disclosing the information reasonably believes that disclosing the information will assist the agency or independent person receiving the information to carry out any of the purposes described in section 66C of the Oranga Tamariki Act.

87 The Oranga Tamariki Act also contemplates a list of other specific reasons where Oranga Tamariki is permitted to disclose information. Oranga Tamariki is permitted to disclose information if it reasonably believes that providing the information will fulfil any of a number of purposes, such as preventing or reducing the risk of a child or young person being subject to harm, ill-treatment, abuse, neglect, or deprivation.[26]

88 Due to the functions of Oranga Tamariki, there may be situations where it believes, on reasonable grounds, that the use and/or disclosure of the information for another purpose is necessary to prevent or lessen a serious threat to life or health of the individual concerned or another individual. For this reason, the Oranga Tamariki Act expressly provides that if there is any inconsistency between the Oranga Tamariki Act and the Privacy Act, sections 66 to 66P of the Oranga Tamariki Act prevail.[27] As discussed above, this means that information use and disclosure that are permitted by the Oranga Tamariki Act will also be authorised by IPPs 10 and 11 of the Privacy Act.

89 Also relevant is the FVA, which allows Oranga Tamariki to use and disclose (to certain agencies) information to:[28]

a make, or contribute to, a family violence risk or need assessment;

b make, or contribute to the making or carrying out of, a decision or plan that is related to, or that arises from or responds to, family violence; or

c help ensure that a victim is protected from family violence.

90 In deciding whether to disclose information in the above circumstances, Oranga Tamariki must have regard to the principle that helping to ensure a victim is protected from family violence should take precedence over both:[29]

a any applicable duty to keep the information confidential; and

b any applicable limit under IPPs 11 or 12 of the Privacy Act on the disclosure of the information.

[25] Oranga Tamariki Act 1989, s 66C(a).
[26] Oranga Tamariki Act 1989, s 66C(b).
[27] Oranga Tamariki Act 1989, s 66Q.
[28] Family Violence Act 2018, s 20.
[29] Family Violence Act 2018, s 21.

Privacy breaches and interferences with privacy

91 The Privacy Act defines a 'privacy breach' as:[30]

a unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information; or

b any action that prevents the agency from accessing the information on either a temporary or permanent basis,

whether or not caused by a person inside or outside of Oranga Tamariki, or attributable in whole or part to any action by Oranga Tamariki, or ongoing.

92 A privacy breach is therefore broader than the unauthorised disclosure of information to a third party. A breach may also involve unauthorised disclosure within Oranga Tamariki, for example, if there is unauthorised access to personal information by an employee ('employee browsing') or the unauthorised sharing of client information between kaimahi.

93 Not all privacy breaches will trigger notification requirements under the Privacy Act. A privacy breach is notifiable for the purposes of the Privacy Act if it is reasonable to believe that the breach has caused 'serious harm' to an affected individual, or is likely to do so. Part 6 of the Privacy Act provides for a 'notifiable privacy breach' regime which requires Oranga Tamariki to, in the event of a notifiable privacy breach, notify the Privacy Commissioner and the affected individuals (or in some cases, give public notice).[31]

94 However, actions that breach the IPPs but do not meet the notifiable privacy breach threshold still cause harm. It is still very real and possible that actions that breach any of the IPPs may cause loss, significant injury to feelings, humiliation, and damage to affected individuals, and therefore may amount to an interference with the privacy of those affected individuals. While unauthorised access, disclosure, alteration or loss of personal information is technically defined as a privacy breach, all other breaches of the IPPs may lead to an interference with the privacy of the individual.[32]

95 Oranga Tamariki must make notifications for notifiable privacy breaches as soon as reasonably practicable. In the case of notification to the Privacy Commissioner, in most cases, this means notifying the Privacy Commissioner within 72 hours after becoming aware of the breach. However, notification to affected individuals is not required:[33]

a if notification would endanger the safety of any person;

b in the case of an affected individual under the age of 16, I notification would be contrary to that individual's interests; or

c if, after consultation with the individual's health practitioner (where practicable), Oranga Tamariki believes the notification would be likely to prejudice the health of the individual.

Complying with the Privacy Act

96 It is not uncommon for those who are subject to the Privacy Act to regard it as complex or troublesome. However, for Oranga Tamariki the Privacy Act aligns with the agency's primary statute, the Oranga Tamariki Act. In both cases the law requires kaimahi to act in the best interests of the vulnerable children and young people they are there to protect. To understand the Privacy Act kaimahi need only acknowledge that a child and their personal information are indivisible. Protecting one will effectively protect the other. However, tensions do exist between the Privacy Act and the

[30] Privacy Act 2020, s 112.
[31] Privacy Act 2020, ss 114 and 115.
[32] Privacy Act 2020, s 69.
[33] Privacy Act 2020, s 116.

Oranga Tamariki Act. The Oranga Tamariki Act makes it clear that the focus is on children and young people, whereas the Privacy Act applies to individuals generally (of all ages). It appears that Oranga Tamariki kaimahi interpret this as requiring a greater focus on the privacy rights of children and young people compared to the adults in a child or young person’s life. Privacy breaches by Oranga Tamariki are more commonly breaches of the privacy of an adult, rather than a child or young person.

How Oranga Tamariki manages personal information

97 Oranga Tamariki is a large organisation with more than 5,000 permanent and fixed term kaimahi at the time this report was prepared.[34] Of those permanent and fixed term kaimahi, 1,714 are social workers. In addition to the core workforce Oranga Tamariki also engages contractors, consultants and service providers as well as a small number of individuals from NGOs and community groups. In total, 9,307 people have Oranga Tamariki logins, meaning they have access to information held by Oranga Tamariki.

98 The core functions of Oranga Tamariki require kaimahi to collect, use and disclose personal information as part of the everyday work of the organisation. To this end, privacy is indivisible from the work Oranga Tamariki carries out. It permeates every aspect of the organisation, from frontline social work to business functions looking to mitigate risk.

99 This part sets out the systems and policies Oranga Tamariki has in place to manage personal information, including training, monitoring and reporting functions, and accountability mechanisms for kaimahi who breach privacy.

Privacy policies

100 Oranga Tamariki has a total of seventeen documents relating to privacy. These policies and guidelines cover a broad range of topics, but the large volume of documents means they are not accessible to employees and the key messages are unclear. Particular topics are repeated throughout the policies including, but not limited to, the definition of personal information, what is privacy, how to record/manage information, and the privacy incident process.

101 The key topics in the guidelines/policies include:

a what is personal information;

b what is privacy;

c principles of Māori Data Sovereignty;

d how to manage electronic and physical records;

e how to protect information;

f what a privacy incident is, and what should you do if you suspect there has been a privacy incident;

g what process should be followed if there has been a privacy incident;

h the roles and responsibilities regarding privacy at OT; and

i how to determine if a privacy review is required.

102 There is no mention in the policies and guidelines of the personal consequences of reporting a near miss or privacy incident. Creating a culture of reporting requires setting out clear guidelines on what will happen, and what protections an employee has when reporting.

103 A breakdown of each of the privacy policies and what they cover is included as Appendix A.

104 The Oranga Tamariki Privacy Policy is the main document which sets out how Oranga Tamariki ‘ensures that it treats the information it collects, holds, uses and shares, lawfully, respectfully and with care.’ Relevant policy statements include:

[34] The headcount as at February 2024 was 5,061 permanent and fixed-term kaimahi, and 5,835 kaimahi in total including casual workers and contractors.

a ensuring that the handling of personal information by Oranga Tamariki complies with the 13 IPPs set out in the Privacy Act. The IPPs are considered to be the foundation of good privacy protocols;

b in applying these principles, Oranga Tamariki will ensure full consideration of its obligations under te Tiriti o Waitangi and section 7AA of the Oranga Tamariki Act;

c Oranga Tamariki kaimahi will promptly report privacy incidents resulting from unauthorised access to, collection, use, or disclosure of personal information to the Oranga Tamariki privacy team, who will determine whether the incident needs to be reported to the OPC; and

d when reviewing, changing, adopting or developing new systems, processes, or services that collect, use, and/or store personal information (including the engagement of a third-party provider), kaimahi will consider potential privacy risks and engage with the privacy team.

105 The document also sets out the key roles and responsibilities relating to the Privacy Policy. Measures of the success of the Privacy Policy include the number of privacy incidents, including breaches notifiable to the OPC, number and type of privacy complaints received and training module completions.

106 Similarly, the Privacy Guidelines is a policy which is intended to be read alongside the Oranga Tamariki Privacy Policy and ‘provide a holistic view of the Ministry’s approach to privacy’. The Guidelines step through every IPP in the Privacy Act and explain with reference to the language used in the Privacy Act how personal information should be collected, used, and stored. However, the specific information sharing provisions of the Oranga Tamariki Act are not set out in the Guidelines. Rather, the reader is directed to another policy for more information on how the Oranga Tamariki Act interacts with the Privacy Act.

107 On the whole, the policies and guidelines provide a comprehensive overview. Further, the Privacy Guidelines define a ‘privacy incident’ more broadly, as being any breach of any of the IPPs. However, one individual we spoke to said that while kaimahi complete privacy training, most do not have any appreciation of the guidelines or policies. This is likely because despite the fact that the policies and guidelines are available to all kaimahi on the Oranga Tamariki intranet, they are repetitive, overwhelming in quantity, not easily accessible, and do not provide clear answers to many everyday issues faced by Oranga Tamariki kaimahi.

Systems

108 When it comes to privacy breaches with a risk of harm, Oranga Tamariki has practical and effective systems in place to deal with the fallout when breaches occur, including dealing with physical security risks and relocation of vulnerable individuals or whānau. However, the systems that would prevent privacy breaches occurring in the first place are hard to identify and kaimahi consider them ineffective.

109 Oranga Tamariki relies on a number of information management systems, principally CYRAS (which is approximately 25 years old) and CGIS (Caregiver Information System, introduced approximately five years ago). Both systems rely on social workers (mainly) inputting information about children, young people, their whānau and carers into the system and updating the files constantly. Any information received from other agencies, medical professionals, schools, the Department of Corrections etc is also inputted into CYRAS, sometimes as attached and scanned PDFs.

110 Oranga Tamariki does have a system for limiting access to files on CYRAS and CGIS, but this is only lightly applied in practice. For example, almost all roles outside of head office have open access to CYRAS, and there is limited functionality for restricting access to particular files or folders within files. Any kaimahi with access to CYRAS will have access to almost all personal information held about almost all children and young people in the care of Oranga Tamariki.

111 Kaimahi are onboarded to these systems via the recruitment process, which includes police vetting. Multi factor authentication – username plus a phone or token – is needed to access an Oranga Tamariki laptop. Further, before a staff member is given access to CYRAS, a 'CYRAS check' is carried out by senior admin staff to assess whether any conflict of interest exists (i.e. a staff member has family members on the database). If an employment offer is progressed then these files are made confidential which prevents the staff member from being able to view case details where a conflict or potential conflict exists.

112 We were told that CYRAS has the capability to provide graduated security levels, which would block access to more files from more eyes, but the agency has opted not to introduce this.

Access minimisation

113 Oranga Tamariki has a total of 1,976,907 'cases' on file. Of these, only 11,315 have at least some aspects of the file restricted and just 8,477 are completely confidential. As noted above, we understand that 9,307 people have Oranga Tamariki logins and there are 3,950 users with access to CYRAS (including both Oranga Tamariki kaimahi and non-employees).

114 The very large number of individuals with access to personal information is a red flag for data protection and yet only 0.6% of the total case files held by Oranga Tamariki have some aspect marked as confidential.

115 Oranga Tamariki says it treats any child and caregiver personal information as 'sensitive' in accordance with the NZ Government Information Classifications. In practice, however, the lack of effective and routine access minimisation means only a very low level of protection is provided to the vast majority of information held and regularly accessed. This is inherently risky. We would expect any of the following cases to be treated as confidential:

a any case that is the subject of media coverage;

b any case that involves a high profile or sensitive / emotionally charged criminal proceeding;

c any case involving a high profile individual or linked (through whānau) to a high profile individual;

d any case which is the subject of political debate; and

e any case with any familial link to a staff member.

116 In addition, other cases which would not meet those thresholds still warrant greater protection than currently exists and we see no reason why access minimisation barriers could not be routinely applied. Applying a graduated approach to access would see kaimahi who deal with information requests, processing of records of concerns, or other triage type work having the greatest level of access. For these workers there can be no predictability about what files they might need to access on any given day. But there is no reason why a frontline social worker should have unrestricted access to files beyond those which are part of their allocated case load and even within an individual's file not all information held needs to be immediately accessible. Where additional information is needed on any file or an additional file is needed (beyond the social worker's usual allocated cases) this should be requested from a supervisor or Oranga Tamariki staff member with more authority.

117 Such access discipline would provide a real action reminder of the sanctity of personal information and the protection it requires. Alternately, the current lack of technological tools such as confidentiality locks is a manifestation of the high-trust / low-accountability privacy culture. Kaimahi defended the status quo in interviews, but principally because this 'is how things have always been done'.

118 However, Oranga Tamariki can and does manage other personal information differently. Under section 23 of the Adoption Act 1955 once an adoption order has been made the adoption record 'shall not be open for inspection'.[35] In practice this means for adoption files only designated staff are able to access any documents (in CYRAS or otherwise stored in hard copy).

119 We see significant advantages in introducing access barriers across all files to minimise access to personal information, for the benefit of children and young people, the adults associated with them, and for kaimahi.

Access to laptops

120 All frontline kaimahi are provided with or have access to laptops and all but approximately 300 Oranga Tamariki staff have a dedicated laptop. Each laptop has a password protection mechanism.

121 However, we were also informed that Oranga Tamariki laptops are or have been provided to community centres and partner agencies in regions where Oranga Tamariki has partnered with others to assist with the provision of care services. Oranga Tamariki appears to have no systems in place to identity which non-Oranga Tamariki kaimahi have access to a laptop, where these laptops are located around New Zealand, or even how many laptops are at partner agencies or community centres. This presents a clear and significant risk. These laptops have the ability to access CYRAS, the largest information management platform and database used by Oranga Tamariki. With potentially unrestricted access to personal information, any unknown individual with the login details for a laptop would have the ability to access the thousands of highly sensitive records held by Oranga Tamariki on children, young people and whānau. Further, we understand that limited contractual mechanisms exist with external parties which provide for adequate or explicit requirements around data management and privacy. While we understand rectification of this is underway, it presents another legal risk for Oranga Tamariki.

Training

122 Oranga Tamariki has four training modules relating to privacy. These are:

a the employee browsing module;

b privacy at Oranga Tamariki;

c an information sharing module; and

d a PowerPoint on data privacy.

123 These modules are all presented online-based. We were told that kaimahi are required to complete the privacy module, but received differing accounts for when completion was required. Kaimahi we interviewed understood that the privacy training had to be completed within the first six months after commencing employment at Oranga Tamariki, while others understood it to be within the first four weeks of commencing employment. Notwithstanding this point of uncertainty, yearly privacy refresher training is compulsory. Frontline kaimahi are also required to complete the information sharing module, and all kaimahi were required to complete the employee browsing module in 2023. There is also:

a an induction for all social workers which addresses privacy (Puāwai);

b an information security module; and

c function specific training in some areas, such as adoption services.

124 The compulsory privacy module training has an 85% completion rate, which is high. However, for an organisation with 5,835 kaimahi, this still means 876 individuals have not completed the training. We

[35] Adoption Act 1955, s 23.

also understand that refresher training is recommended in cases where individual staff have showed a lack of understanding of privacy. However, without a compliance function, there is no way to ensure that this occurs.

125 The privacy team at Oranga Tamariki have successfully modified their approach to staff to drive compliance with privacy training. The objectives of the module are that by the end, the user will 'have a high-level understanding of privacy, including what personal information is, the information life cycle, how privacy considerations should be woven into work, and how to prevent and/or manage privacy incidents'.

126 One part of the privacy module states that there must be safeguards to prevent loss or disclosure of information, 'including limits on who can access it based on their roles. To support our obligations, you should flag or mark files and pieces of information as appropriate (e.g. confidential).' We discuss confidential files above at 113 - 117 but in short, this practice is not routinely applied.

127 Further, the privacy training module states that personal information should only be used for the purpose it was collected or a directly related purpose. While this is the language used in the Privacy Act, it is overly legalistic for all staff privacy training. The same issues apply to the sharing and disposal of information modules, which merely recite the language of the Privacy Act. Legalistic language makes training inaccessible for those unfamiliar with privacy law, or legal language, who typically will need plain language guidance about what specific terms such as 'purpose' or 'directly related purpose' mean.

128 Further, the 'real world' scenarios in the training module only relate to privacy breaches or specifically, what the likely harm caused by a privacy breach is. There is no scenario type training which would go to the prevention of privacy breaches, such as examples of when information may be lawfully used or disclosed. It is often relatively straightforward to identify the possible harm following a breach (e.g. a threat to physical safety when giving an address which is subject to a protection order) but it is less obvious when some types of information should be used or shared (or if there is no valid basis for that information's use or disclosure).

129 Feedback from the employee browsing module provides good guidance on what is needed across all training modules. Specifically, kaimahi wanted:

a more training in disclosure of information, such as sharing aspects of a report that is not public;

b more clarity around consequences, particularly what happens when there is a privacy breach and whether this is different for various parts of the organisation;

c training on discussions in office and when conversations should be taken to a meeting room;

d training on what may constitute a less obvious privacy breach e.g. uploading documents to the Oranga Tamariki intranet;

e guidance on interdepartmental disclosure of information within Oranga Tamariki; and

f guidance on requests for sharing information in response to an informal request from emergency services such as Police or hospitals.[36]

130 The above demonstrates the range of complex questions faced by Oranga Tamariki on a daily basis. While the privacy training modules include examples of common scenarios that require privacy considerations, these scenarios are simplified and aimed at entry level privacy considerations. The feedback was that they did not provide sufficient information on the kind of difficult issues facing kaimahi, nor were they presented in a way that kaimahi considered relevant or engaging. In

[36] "Requests for sharing information from an NGO, if this is done in an informal manner with a phone call from a friend who works at an NGO wanting to know if there is Oranga Tamariki involvement for a tamariki/whanau they are concerned about. It would be good to have a specific example around this. Even if someone from the Police or Hospital contact a Social Worker informally to request information" Oranga Tamariki *Feedback - Employee Browsing Evaluation* (6 October 2023).

response, Oranga Tamariki managers said the modules are deliberately generic because they are designed for kaimahi across the whole organisation.

Monitoring

131 Oranga Tamariki has minimal monitoring of its systems and practices. Oranga Tamariki does not have a compliance team, and while multiple people in the organisation have some responsibility for privacy, there is no cohesive system for ensuring privacy policies are followed and the Privacy Act complied with. We understand that while a compliance framework has been recently approved, it has not yet been put in place due to resource constraints. We have not seen a copy of the proposed framework. This lack of proper monitoring means Oranga Tamariki does not have a complete picture of its own privacy culture. In short, it cannot know what it does not know.

132 The privacy team and others have been active in trying to increase visibility of privacy. The drive to reach 85% completion rates on the annual online training module is evidence of this. But largely the organisation relies on people to do the right thing when a breach or a suspected breach occurs to prompt any review or checking.

133 For example, where inappropriate access to a file is alleged or suspected, a ‘footprint’ check may be conducted and an investigation commenced if necessary. This footprint report displays all users who have accessed a particular file and when the file was accessed. Reports of this kind are extremely informative, but at Oranga Tamariki footprint reports are available on request only. There is no proactive auditing of access to CYRAS and spot checks are not done. This applies to employee browsing of files. Oranga Tamariki cannot give any assurances that kaimahi do not browse in files they have no authority to read because no random checking is carried out. Staff members we spoke to described footprint reports as ‘reactive’ and described a cultural resistance to random monitoring of access to CYRAS.

134 One staff member said:

> *There is nothing proactive or holistically detective around the monitoring of access to CYRAS and obviously that is some of the most sensitive information that the organisation holds.*

135 It was evident from the interviews conducted with Oranga Tamariki kaimahi that the lack of monitoring and oversight is not limited to CYRAS access, but extends to other areas of the organisation. Kaimahi indicated that there is also no monitoring of the implementation of controls or recommendations from privacy impact assessments (**PIAs**). The effect of this is that Oranga Tamariki is unaware of what privacy mitigations from these PIAs it actually has in place and what risks it is still exposed to.

Reporting

136 Serious privacy breaches, which meet the threshold for notification to the OPC, are reported, followed up and addressed. But the overall reporting of privacy breaches is incomplete. Kaimahi told us, in no uncertain terms, not all breaches are reported. One Oranga Tamariki staff member interviewed said:

> *There was an example a couple of months ago where someone requested some advice from me and they told me what had happened and I was like ‘have you consulted with the Privacy Team, it looks like this might be a privacy breach?’ and they just hadn’t turned their mind to it at all.*

137 Many kaimahi appear to have either a lack of awareness about what constitutes a breach of privacy or a lack of awareness about what processes and supports are in place at Oranga Tamariki. The effect of this is they either do not recognise a breach or they do not report it. Self-reporting of near misses and privacy breaches is uncommon. Given the lack of monitoring this is hardly unsurprising,

although kaimahi from different parts of the business had different perceptions of self-reporting. It may be in some sites, where managers are motivated to improve privacy, reporting is more proactive but we did not see evidence of this in the information provided for this review.

138 Other kaimahi stated that accountability concerns meant there was a culture of fear about reporting a privacy breach. There have been disciplinary procedures launched as a result of some privacy breaches. Inevitably, that could have a chilling effect on co-workers. Nonetheless, employees need certainty about what will happen to them following a breach, and what protections they have when reporting. Those working most closely in privacy at Oranga Tamariki would like to see the development of near miss reporting as an educative tool but the organisation falls well short of that ideal currently.

139 Overall, because Oranga Tamariki does not have an accurate picture of all breaches it cannot identify patterns or the causation of breaches that fall below the notifiable ‘likely to cause serious harm’ threshold. However, where notifiable privacy breaches occur they are generally reported to the OPC within 72 hours of Oranga Tamariki becoming aware of the occurrence of the privacy breach, as recommended by OPC guidance.[37]

Accountability

140 Accountability for privacy breaches within Oranga Tamariki is mixed. Multiple Oranga Tamariki kaimahi interviewed indicated that it is unclear whether a privacy breach will be a disciplinary matter or not.

141 Part of this stems from Oranga Tamariki having an emphasis as an organisation on education rather than compliance. Enforcement of disciplinary action for privacy breaches therefore varies depending on the nature of the breach, but also on the particular manager or team lead. One manager interviewed as part of this review stated that they deliberately do not tell their staff when they have breached privacy.

142 This practice stems from that manager’s preference for an educational rather than disciplinary response, but also out of concern that staff members will over-correct once they learn they have caused a privacy breach. From the manager’s perspective, informing kaimahi they have breached privacy risks that staff member becoming too conservative when information should be disclosed.

143 The fact that accountability is inconsistent throughout the organisation is reinforced by the following statements from various Oranga Tamariki kaimahi:

> *[Privacy breaches] come from a lack of understanding and a lack of confidence and practice and making those professional judgements and feeling safe to be able to do so.*
>
> *We are inconsistent from a HR perspective of how we deal with these [privacy breaches].*
>
> *The [privacy breach] that I am thinking about was kind of rough because it was very much structural tiered and then the person at the bottom [copped it].*

144 Consistent and transparent accountability processes would reinforce the importance of privacy, but also give Oranga Tamariki kaimahi the confidence needed to effectively carry out their day-to-day work. An uncertain approach to disciplinary action only encourages kaimahi to withhold information to the potential detriment of children and young people, or on the flip, be too liberal with the use and sharing of personal information if there are no consequences to actions.

145 Accountability ultimately requires clear organisational structure and leadership. It is not clear who is leading the privacy initiatives at Oranga Tamariki. In reality, a number of mid and lower tier managers have key roles but work in siloes rather than in any integrated or joined-up way. This

[37] With the exception of two breaches from 2022 which were reported outside of this time period, as it was some time from the breach occurring before Oranga Tamariki could confirm that a notifiable breach had in fact occurred.

makes it difficult for other kaimahi to recognise who has authority and / or who to consult. It also makes it difficult for any manager to drive change and improved performance.

146 In respect of performance, the active involvement of the OPC has and is impacting on how Oranga Tamariki responds to serious breaches and those affected by them. But it is not clear that any other part of the business has clear performance targets either to work towards or to report on. The lack of performance targets is likely to influence the overall lack of data on privacy and information management.

Role of the privacy team in Oranga Tamariki

147 Privacy at Oranga Tamariki is managed by a specific privacy team but also by others in the organisation, each with a varying degree of responsibility for privacy. This leaves plenty of room for confusion about whose job it is to deal with compliance enforcement or who has the mandate to address particular privacy issues.

148 The privacy team was established in 2018 following the separation of Oranga Tamariki from the Ministry of Social Development. Since this time the privacy team has developed a suite of policies and guidance, created and implemented mandatory trainings, and worked to raise overall privacy awareness in an organisation of over 5,000 people.

149 This is no easy task, particularly given the educative, largely informal and high-trust culture within which Oranga Tamariki operates. In the first year or so, the privacy team focused on building visibility, including the development of organisation charts to help formalise the relationships between teams with privacy and other incident reporting responsibilities. This assisted in creating informal reporting channels with other teams, such HR and operations, in order to ensure that processes were in place for escalating and responding to privacy breaches.

150 To the extent that the privacy culture at Oranga Tamariki has shortcomings this is not the fault of the privacy team. The agency's issues are systemic and cultural.

Structure of the privacy team

151 The privacy team are individuals who report to a tier four leader (the Chief Information Security Officer). At tier four, the Chief Information Security Officer is not part of the leadership team at Oranga Tamariki. This impacts the privacy team's ability to command authority and to drive cultural change. Its function appears to be limited to being an advisor to the rest of the business. Notwithstanding the fact that the privacy team has a good reputation amongst National Office, it faces an uphill battle in terms of championing change amongst Oranga Tamariki more broadly.

152 There are three roles in the privacy team: lead advisor, senior advisor, and advisor. In each case the job descriptions are vague and lack any specific measure of accountability. For example:

a for the lead advisor, a key accountability measure is to 'deliver results by making things happen with and through others'. Other capabilities for the lead advisor include to 'lead and engage with others in ways that help [Oranga Tamariki] navigate the future'.

b the senior privacy advisor includes accountabilities such as 'provide specialist advice and support to Oranga Tamariki to embed increasingly mature privacy practices and frameworks'.

c the advisor's role is to provide 'specialist advice to Oranga Tamariki kaimahi on the management of data, information, privacy and records to ensure information is managed as an asset'.

153 None of the three position descriptions specify who is responsible for compliance, monitoring or assurance, but all can be read one of two ways: either that the privacy team has complete

responsibility for putting privacy into practice, or no one has responsibility. In practice, it works the second way.

154 One example of this is the lack of compliance monitoring following a privacy impact assessment. PIAs are a tool used by agencies to help identify and assess the privacy risks arising from a particular project, software, or proposal which results in the collection, use or handling of personal information. PIAs also usually propose ways to mitigate or minimise privacy risks, making PIAs an essential element of an organisation's risk management toolkit.

155 As part of their workplan for 2023, the privacy team created a document which listed every PIA commissioned by Oranga Tamariki, as well as the recommended controls and privacy mitigations needed for each project. This document has over 600 entries and dates back to 2016. However, no protocol exists to follow up with these controls to ensure they have actually been implemented and the baton of responsibility seems to be passed from team to team.

156 While it would be reasonable to think this compliance work should be done by the privacy team, we were told it would more likely fall within the mandate of risk and assurance. The privacy team has neither the resource nor the remit to do compliance work and as a tier four team, we consider its authority is heavily limited.

So whose job is compliance?

157 The decentralisation of privacy at Oranga Tamariki means that it is hard for the privacy team to have direct access to frontline practice where many of the privacy breaches occur. Oranga Tamariki is structured so that the business operations and service delivery teams generally have oversight of the Oranga Tamariki sites (and by extension, social workers). In the event of a privacy breach, this means that the privacy team sometimes has to go through three middle managers to find out the circumstances of the breach and the likelihood of potential harm occurring.

158 As the privacy team has limited authority, it does not have the mana nor the resourcing to carry out privacy compliance, monitoring or assurance activities. For example, we were told that following a privacy breach at an Oranga Tamariki site, it was discovered that the majority of kaimahi at that site had not completed the mandatory privacy training. However, the privacy team was unable to take enforcement action themselves, and instead were told that the executive manager at the site would take care of it. While it is unclear whether compliance is even within the privacy team's ambit, the team has not been given any tools which would enable it to operate effectively and with the authority it needs to function within the organisation.

159 As a result, the privacy team has worked on relationship building with various other teams within Oranga Tamariki and has created a series of informal reporting channels where formal systems are lacking. For example, the feedback and complaints team loops the privacy team in when the organisation receives a complaint with a privacy element, even if that complaint has not yet been investigated by Oranga Tamariki. These processes enhance the visibility of the privacy team, but are reliant solely on the privacy team maintaining good relationships with other teams. This is an ad hoc and risky way to manage privacy.

Reporting up

160 It is unclear where the onus lies for the reporting of breaches happening at the frontline site level. Notwithstanding the privacy team's best efforts, it still struggles to gain visibility amongst kaimahi and the various regional sites.

161 The team uses the agency's intranet system to communicate across the country. However, we heard from kaimahi who simply did not engage with the policies and updates this way. Some kaimahi, we were told, could not or did not use the intranet communications system, Te Pae. Since the policies

and notifications about privacy are published on Te Pae this represents a major barrier, outside the control of the privacy team.

162 Unsurprisingly, the lack of visibility and bureaucratic organisational structure means that the privacy team is not the first port of call for kaimahi who breach privacy. A breach from a frontline staff member would first be reported to the site manager, who reports to an executive manager, who reports to a regional manager, who reports up to the operations team, who then loop in the privacy team.

163 Sitting at the end of this chain means that the privacy team are only actually notified of a breach by the time that the information has been passed to potentially upwards of five individuals. This naturally restricts the ability of the privacy team to effectively undertake compliance and assurance activities, or ascertain what has actually happened following a privacy breach.

Breaches of privacy

What is a breach of privacy?

164 There are no grounds for confusion about what constitutes a breach of privacy.

165 The Privacy Act defines a breach as unauthorised or accidental access to, or disclosure, alteration, loss or destruction of personal information.[38]

166 An agency such as Oranga Tamariki must notify the Privacy Commissioner as soon as practicable after becoming aware that a *notifiable* privacy breach has occurred. A notifiable privacy breach means a privacy breach that it is reasonable to believe has caused serious harm to an affected individual or individuals or is likely to do so.

167 This review was prompted by the OPC receiving an unusual number of notified breach reports from Oranga Tamariki. Records show that between January 2021 and December 2023 it notified more than 30 separate breaches. We received no information about how many, if any, other privacy breaches were identified that did not meet the threshold for notification. A copy of the agency's privacy 'incident' tracker, identifies 595 incidents since 2019, at an average of 9 per month.

168 Those that were notified, included the following:

a sensitive notes from an interview including allegations of abuse against the mother of a child were sent to the child's grandmother;

b information about a child was inappropriately accessed by a staff member and provided to the staff member's family;

c a social worker shared the identity of an alleged abuser from historic and unsubstantiated claims with the man's whānau and others;

d the identity of a person who had made a report of concern (**ROC**) about a child was shared with family members as the individual's personal information was included unnecessarily in court documents;

e a staff member took a screenshot of a mother's file and shared it with the child's father. In this case, the disclosure allegedly led to further physical abuse of the child's mother;

f a family group conference (**FGC**) concerning the welfare of a young person was secretly recorded. A video of the young person addressing those attending was then published online;

g a social worker gave the address of a child and their mother to the child's father who was on bail at the time for the alleged rape of a young person living with the mother;

h multiple copies of client files were found by a road worker in rubbish left in Ngauranga Gorge. The patient files had been incorrectly disposed of by a psychologist; and

i a locked cabinet was donated to a charity organisation. The cabinet contained client and HR files about Oranga Tamariki employees. The HR files were subsequently thrown into a skip by a charity worker who notified an affected employee's family member.

169 These examples represent just a snapshot of how personal information has been managed and disclosed. In some cases the person responsible was a staff member, but not always. In some cases the disclosure was inadvertent, but again not always. Regardless, each case represents a grievous breach, particularly given the nature of the information held by Oranga Tamariki, the vulnerability of the children and young people involved and the volatility and fragility of their circumstances. The

[38] Privacy Act 2020, s 112(1).

Deputy Privacy Commissioner described some of the breaches as the worst she had seen, given the risk disclosure of this personal information poses to the individuals involved.

170 In the cases cited above unauthorised and inappropriate access and disclosure of personal information put children and others at real risk of physical harm, which in some cases actually occurred.

171 There is no question that kaimahi recognise this danger. A number of those we interviewed said they worried that people would be harmed as a result of poor personal information management. Where they were aware of breaches, they spoke of acting quickly to help those affected or potentially affected.

172 To that end, the agency has a well-established set of protocols for responding quickly and effectively when it thinks a breach of privacy may put a child or young person and / or members of their whānau at risk. This includes relocating a family, liaising with police and / or installing security alarms at a residence. But such responses are quite literally an ambulance at the bottom of the cliff. It was telling that kaimahi involved in these post-release interventions did not see compliance with the Privacy Act as having any particular relevance to their roles.

Is there a pattern to who breaches privacy and how?

173 Of the more than 30 notified breaches since 2021:

a 19 were the result of actions taken by 'service delivery staff', principally social workers;

b 1 was a staff clerical error at National Office, involving the release of payroll information;

c 6 were the result of actions taken by third party providers who work with Oranga Tamariki; and

d 7 were the result of errors made by staff processing information requests, often requests made under the Privacy Act.

174 We recognise that from time to time mistakes will be made. In particular, we consider the work the customer information requests response team (**CIR**) does replying to information requests is especially vulnerable to human error.

175 Anyone is entitled to make a request under section 40 of the Privacy Act for access to their personal information held by the agency. Oranga Tamariki receives as many as 895 such requests each month, typically from individuals who were formerly under the care of Oranga Tamariki or its predecessors. The files held on these individuals can be substantial. We were told of one file which ran to 30,000 pages of documents. Because the files contain personal information about others (and not just the requester) each file is redacted to remove the names or personal information of other individuals prior to release. This is a time consuming task, with the redactions being applied manually by a staff member. Given that many of the pages are scanned prior to upload to Oranga Tamariki IT systems, technological aids which could catch any missed redactions (such as the ability to search for names) are not able to be used. With potentially many hundreds (or even more) redactions applied to each request this leaves ample room for human error. That cannot excuse the breaches, however. We were also told, due to capacity issues, the redactions of any release are not checked by a second pair of eyes, which would be good practice and could also pick up missed redactions.

176 We were also told that while Oranga Tamariki primarily uses information management software (such as CYRAS and CGIS) to keep digital files, the organisation also holds large volumes of paper files. Privacy issues relating to these files involve inappropriate storage, failure to redact information when releasing, and accuracy issues given the fact many paper files are historical records.

177 For the most part the notifiable breaches occur while kaimahi carry out routine daily tasks and most commonly they relate to the personal information of adults, rather than children and young people.[39] In a small number of cases, the inappropriate disclosure of personal information appears to have been deliberate (e.g. when a social worker shared the identity of an alleged abuser with his whānau or when a social worker inappropriately accessed files to provide information to her own family). Deliberate breaches are or ought to be a disciplinary issue. But in most cases the breaches appear to be the result of poor practices and / or a lack of understanding about the management and disclosure of personal information. In some cases, the breach was due to a lack of care. The failure to check whether a locked cabinet contained any files before it was gifted to a third party is a clear example of this. In that case, the breach could easily have been avoided by applying nothing more than common sense.

178 During the course of our interviews it was evident that, across the motu, social workers do vital work in difficult circumstances. Universally they carry heavy caseloads. The strain of this will affect how they manage their clients' information and the time they have to make thoughtful decisions about information sharing and disclosure, particularly when under pressure.

179 In one of the notified breaches, for example, a social worker under duress from a child's mother provided her with the address of the child's father. In the particular circumstances, this was an inappropriate release of personal information, and potentially dangerous. Any social worker in those circumstances requires support and processes on which they can rely to de-escalate the situation including, if necessary, having another social worker step in to manage communications with the mother and / or other members of the whānau. In practice, however, we were told social workers managing multiple cases with complex clients commonly perceive privacy as an add-on which complicates their interactions.

180 Accepting social workers have challenging roles, the complexity of their working practices do not exempt them from complying with the Privacy Act. Troublingly, it was evident from a number of interviewees that these obligations are regarded as not as important as their primary role.

> *To remove a child or not from a parent I would argue is a bigger decision than a privacy breach because literally children die. If social workers take particular action - it doesn't matter what that action is - if we take an action and we remove a child that is a bad result because then we have stolen a child. If we don't take the child and the child dies we have failed everybody because we didn't protect the child.*
>
> *Those are the decisions that social workers are facing every single day and whether or not there is a small privacy thing that is not front of mind.*
>
> *Front of mind is this child could die. If it dies, I will be on the front page of the media. There will be a review into my practice to say that I have failed. I won't be named but if you read any practice review the social workers are hung out to dry. That is the reality for social workers at the frontline. Privacy is not front of mind for them. It is in there somewhere.*
>
> *We are not minimising privacy breaches but the reality of any social worker at the frontline is that there are so many competing priorities and fundamentally we are trying to keep kids alive. We are trying to keep families together. That is the priority.*

181 This mindset is hugely influential in how kaimahi at Oranga Tamariki deal with personal information. So too, is the strong focus on what was described as a 'trust others, so they will trust you' approach to whānau and their personal information. The obvious confusion that exists around how the Privacy Act works is obvious from feedback that suggested some kaimahi believe any focus on the parts of the Privacy Act that enable information sharing will actually make social workers less willing to share

[39] Oranga Tamarki kaimahi were keen to draw this distinction. However, the Privacy Act affords all individuals the same rights to protection and, in reality, the breach of an adult's personal information by Oranga Tamarki could have profound impacts on a child related to or associated with that adult.

information. Dame Karen Poutasi's 2022 report into the death of five year old Malachi Subecz identified this as a lack of understanding about how the Privacy Act and Oranga Tamariki Act work alongside each other.[40]

182 Fundamentally though, privacy is simply not front of mind for kaimahi. Taken together, and separately, these attitudes illustrate poor practices which have become normalised and accepted. But also, and just as important, not all kaimahi are receptive to change. A common theme from the information gathered as part of this review and those we spoke to was that Oranga Tamariki operates a largely informal and high-trust culture. Attempts to instill accountability or re-educate kaimahi (particularly those at the frontline) have previously been met with resistance and perceived as an attack on competency. Feedback provided to an employee browsing training module feedback gives an insight into how training can be received:

> *I am an experienced social worker and this training has made me feel frustrated and undervalued. I am all for reflective work as this help with my practice but to disrespect the qualifications I have worked hard for is not mana enhancing.*

183 These attitudes present a major challenge.

Do all breaches get reported?

184 Due to the high number of notified breaches, the OPC has taken, and continues to take, a very active interest in compliance by Oranga Tamariki with the Privacy Act. Because of this we are confident that the most serious breaches – those with the potential to cause serious harm – are reported.

185 However, there are issues with the way the agency records and / or categorises breaches. We asked both Oranga Tamariki and the OPC to provide a schedule of notified breaches. As the table (summarising the notified breaches since 2021) below shows, the information provided by the two agencies differs in some respects relating to both the number of recorded breaches and the way each is recorded.

Type of breach	**OPC recorded incidents**	**OT recorded incidents**
Email error - attachment of personal information error	6	4
Email error - wrong recipient	1	1
Loss or theft of physical documents - disposal of equipment error	1	1
Loss or theft of physical documents and IT equipment - vehicle broken into	1	1
Other - documents left lying around	1	2
Other - inaccurate information supplied	1	2
Unauthorised access - employee browsing	1	1
Unauthorised sharing - disclosure of information	5	13
Unauthorised sharing - employee browsing	2	1
Unauthorised sharing - redaction error (including OIA responses)	10	4
Unauthorised sharing - unauthorised recording of group meeting	1	1
Website or IT system error - phishing email	1	1
Website or IT system error - role base permission error	1	1
Total	**32**	**33**

[40] Ensuring strong and effective safety nets to prevent abuse of children, Dame Karen Poutasi, November 2022 at [187].

186 We have not been able to explain the difference in the reports and have informed the OPC about the discrepancies in how the breaches are recorded.

187 Ensuring that each breach is accurately described and recorded is an important part of monitoring privacy breaches which, in turn, is necessary if lessons are to be learned and privacy compliance improved.[41] The way a breach is described also informs how the leadership team understands both the nature of the breach and the seriousness of it.

188 But a larger, more challenging question is whether all privacy breaches are reported and acted on. As noted above, under the Privacy Act only breaches with the potential to cause serious harm need be notified. Because of the nature of the sensitive personal information collected and held by Oranga Tamariki, and the vulnerabilities of the whānau involved, more breaches are likely to meet this statutory threshold than might apply in some other government agencies. However, we were provided with no information indicating Oranga Tamariki has a complete picture of all privacy breaches or near misses across all of its work. To the contrary, we were told by a number of interviewees that they knew not all privacy breaches are reported.

189 There appears to be a number of reasons for this. Firstly, reporting processes are inconsistent across different sites and parts of the organisation and possibly not well understood. Secondly, and importantly, practices routinely breach privacy rights without recognition. Kaimahi we interviewed acknowledged that they had not previously considered their conduct through a privacy lens. As one said:

> *The basic stuff like how many files and names and whiteboards and things just roll through our offices and we have got cleaners trapsing through and workmen and there are conversations being held in the middle of the office*.

190 Some of the specific examples of risky workplace practice identified by interviewees include:

a Personal information is routinely printed out for convenience. We were told of loose papers being left on desks and in common work areas in full sight.

b Kaimahi create PDF documents of some personal information and retain this on their laptops for easy access. There is no system to ensure this information, even if used correctly, is deleted as soon as practicable and no checks to ensure this occurs.

c Some kaimahi use personal phones to record information. As above, there is no system to ensure this information, even if used correctly, is deleted safely.

d Although all kaimahi have access to a laptop, we were told kaimahi routinely take paper files out of the office. We were told of files left in cars or taken to family group conferences and other locations where they may be seen or inadvertently left.

e One youth justice facility has personal information about young people written on white boards in offices that are accessible to third parties, including cleaners.

f When responding to an internal request for information personal information about a child or young person that was not relevant to the specific request was attached and shared with a wide group. No one reported this.

g In one incident minutes of a meeting were shared internally to communicate a policy decision to key staff, but with personal information about a young person attached. This information was not relevant to those at National Office receiving the minutes. Again, no one reported this.

[41] Oranga Tamariki does hold accurate information about notified breaches. The distinction here is how, in any summary or record, it describes and classifies each breach.

191 From what we were told these practices are or were regarded as neither risky nor a breach of privacy, which is wrong on both counts. The practices described above all create opportunities for the unauthorised disclosure of personal information in ways that, intentional or not, could interfere with a person's privacy and could cause harm.

192 They also indicate that kaimahi do not sufficiently appreciate that privacy breaches are not limited to breaches that meet the statutory threshold for notification. Internal processes at Oranga Tamariki may actually reinforce this because while the agency has internal processes in place for notifying and responding to notifiable privacy breaches, there is much less scaffolding for other interferences with privacy. In reality, all breaches ranging from accidentally sending the wrong document to another kaimahi to releasing the details of a record of concern notifier should be reported to the privacy team and all staff need to both understand this and comply. If only some breaches are reported, as seems to be the case, Oranga Tamariki will not have a complete picture of what breaches occur and why. This limits its ability to properly understand its vulnerabilities and risks and effectively target training and support.

193 But achieving an uptake in reporting will require redefining what the organisation views as a privacy breach. Under the Privacy Act, any unauthorised access, disclosure or loss of information is a privacy breach. Any action that breaches any of the IPPs may lead to an interference with privacy. Education is needed to reinforce this point and the message that Oranga Tamariki takes all privacy breaches seriously.

194 It is important to note that improving reporting processes will usually result in an increased number of privacy breaches being reported. Over time it should also result in an increased willingness and likelihood of near misses being reported. In both cases, the agency will need to adjust its thinking to accept that – in the short term at least – more reported breaches is a necessary step to ultimately preventing notifiable breaches.

What is the underlying cause of privacy breaches?

195 As noted above, there are strong cultural factors contributing to how Oranga Tamariki kaimahi manage personal information. These include:

a A general lack of consideration about privacy. Many appear to regard it as a once a year training module which must be completed and then effectively parked. A high number of kaimahi appear to consider privacy to be someone else's responsibility.

b Open access to information, without the effective scaffolding of consistent monitoring, compliance and enforcement. In fact, the prevailing view appeared to be that a compliance approach would hamper the work of the agency.

c A lack of accountability. Working practices routinely appear to breach privacy and yet it was common for kaimahi to explain this as the fault of poor technology, or being too busy to act differently, or because this is how they had always worked. These excuses appear to have been regarded as acceptable.

196 The fact that privacy is simply not front of mind is likely to be the most common cause of privacy breaches. Kaimahi dealing with personal information, even very sensitive personal information, are not sufficiently cognisant of their obligations to protect it and / or how they might do so. They understand the information is sensitive, because they told us so. They also understand some information is more sensitive than other information. But they did not seem to draw the necessary connection between the fact that all personal information is subject to the protections of the Privacy Act and the obligations that apply every time they collect, hold, use or disclose information.

197 One contributing factor may simply be the agency's open gate approach to all information. Personal information is held on a number of computer systems, but most notably CYRAS. The information

stored on CYRAS includes information about every child and young person in the care of Oranga Tamariki. All social workers can access almost all files on the CYRAS system, which is available on their laptops wherever they log in. The system does not contain any graduated gateways distinguishing between more experienced and less experienced kaimahi. It does not limit access according to which social workers and supervisors are assigned to any particular file. Unless a child is adopted or one of a very small number of 'sensitive' clients, almost all frontline social workers can access their file and all information contained in it. We were told that this 'open gate' level of access is required to enable kaimahi to quickly search and locate information relevant to their work. Almost all interviewees defended this approach and some noted that all kaimahi must adhere to the Oranga Tamariki Code of Conduct which covers access to CYRAS. However, we think the balance is tipped too far in favour of permitting easy access to information at the expense of protection of privacy.

198 Further, use of CYRAS is largely unsupervised. There are no random checks to test whether kaimahi are using their privilege of access responsibly. New frontline recruits have access to CYRAS even before they have their formal induction ('Puāwai'), which usually occurs between five weeks to six months after commencing employment (by which time individuals are more familiar with the information management system).

199 This high trust approach obviously makes it easier for social workers (and their supervisors) to do their jobs. A worker with CYRAS access need not ask permission to access a child's file (and all it contains). However, one unintended consequence of such open access may be that it inadvertently sends the wrong message about the importance the agency gives to privacy protection. The default position is that all information is accessible at any time. Social workers are seldom required to justify accessing any file. No one asks the fundamental questions; Do you need to read this? Do you need to share it? In a number of cases we were told about, Oranga Tamariki kaimahi accepted they received or saw more information about children and young people than they 'probably' needed to see. But also, this approach impliedly gives them permission not to think too hard about privacy, including when they share the information with others or are asked to share it.

200 It is certainly evident that insufficient consideration is given to the fact that only those kaimahi with a legitimate purpose should access the personal information of any child, young person or whānau member. Among those we interviewed it was not well understood that work practices, such as those described above, provide an opportunity for others, even co-workers, to read or access the information without authorisation. It may be that multiple social workers and / or supervisors have a reason to access one child's file. But in each case, the individual must be legitimately engaged in some capacity on the child's case and acting in their best interests to be authorised access. Active steps are required to ensure the personal information is protected from anyone else.

201 We heard from kaimahi, at all levels, who (to the extent they considered the Privacy Act) regarded privacy as detached from and different to their core responsibility to children and young people. Such a distinction is incorrect and risky. There is no difference in practical terms between acting in the best interest of the child or young person (as required by the Oranga Tamariki Act) and protecting the privacy of the child or young person and people associated with that child or young person (as required by the Privacy Act). The two sets of responsibilities are completely aligned and interdependent.

202 Concerningly, we were told by one interviewee of social workers who could not see the connection between protecting privacy and protecting the child.

> *They hated it. They couldn't see the connection. If we can connect it up, if we can actually say this about you protecting the mana of these people, this is how you practice. This is not privacy. It is not an Act. It is how you practice. And how you practice is that you think about what do I need to share? Why am I sharing it?*

203 The assessment by Oranga Tamariki of its privacy culture, discussed in more detail later in this report, is that its privacy maturity is improving, with the agency 'striving to go above and beyond legislative requirements'. The number of notified breaches, the seriousness of some of those breaches and the lack of engagement from kaimahi (evidenced in interviews completed for this review) tell a different story. Oranga Tamariki has a low maturity privacy culture. Even after repeated reviews, high profile media criticism of privacy breaches and the introduction of the post-2020 notification regime, many Oranga Tamariki kaimahi still appear to find the Privacy Act either confusing or distracting. If Oranga Tamariki is to prevent further notifiable breaches these attitudes need to be addressed.

204 The reality is if, as has happened, personal information about a child's parent or whereabouts is released to someone who should not have that information then the child or the child's parent may be in emotional or physical danger. Setting aside privacy questions, this is a breach of the paramountcy principle – the need to keep the best interests of the child paramount. In this, no distinction should be drawn between the child and the child's personal information. Both require protection and vigilance. But in all cases protection of the child and protection of the child's personal information are indivisible.

Complaints to the OPC

205 For completeness, we also note that in addition to breaches notified to OPC by Oranga Tamariki, the OPC also received complaints made by individuals. These are not the subject of this review. From 2021 – 2023, 33 total individual complaints were received by the OPC in relation to privacy management at Oranga Tamariki.

206 As the table (summarising the complaints to OPC since 2021) below shows, the majority of complaints related to a failure to provide information in response to a personal information request.

207 These complaints arise from one of the key obligations for any agency under the Privacy Act. While on the one hand the Privacy Act makes it compulsory to protect personal information from unauthorised disclosure, on the other it requires an agency to disclose to any individual the personal information that it holds about them, and to correct any information held which is inaccurate, out of date or misleading. In a large majority of the complaints about responses to such requests, the OPC found that Oranga Tamariki was justified in withholding the information, as it related to the personal information of a third party.

Nature of complaint	**OPC recorded complaints**
Failure to timely respond to personal information request	7
Inaccurate information held	2
Failure to provide information (inappropriate redaction or withholding)	18
Failure to respond to or address access request	2
Unwarranted disclosure of information	4
Total	**33**

208 Of these complaints, three are still under investigation by the OPC. All other complaints have been closed by the OPC. Two were referred to the Human Rights Review Tribunal (**Tribunal**), although one was declined by the Chair of the Tribunal. Six other complaints were picked up by the Tribunal upon application by the complainant.

How Oranga Tamariki rates its own performance

209 In August 2014, the Government Chief Privacy Officer issued the Privacy Maturity Assessment Framework (**PMAF**) to support agencies to meet expectations for good privacy practice and develop privacy maturity. There are four broad categories of expectations for agencies:

a core expectations, including having a people-centred privacy programme, creating a privacy culture, conducing training, implementing privacy practices, and identifying Māori privacy interests;

b leadership, including privacy reporting, responsibility, assurance and oversight;

c planning, policies, and practice; and

d privacy domains, including having a process, knowing the agency's risks, retaining personal information, and minimising the collection of personal information.

210 Agencies complete a PMAF self-assessment to examine privacy capability and maturity of the organisation. There are 42 sub-criteria which fit into the four categories of expectations above. The way that PMAF reports are structured is that each section has its own table which outlines the overall maturity level for that section. There is no one overall maturity level given. The organisation selects the appropriate maturity level for each criteria using the following descriptors: informal (at the lower end), foundational ('basic' prior to 2022), or managed (at the higher end). The organisation then provides a narrative which expands on the reasoning for each rating. The ratings are described as:

a informal – the agency's approach to privacy is unstructured, privacy is generally seen as a compliance exercise, and planning / implementing the privacy work programme needs to be developed;

b foundational / basic – an agency wide approach to privacy is developing, good privacy practices are siloed, happening at the individual initiative and team level rather than agency-wide; and

c managed – the agency's approach to privacy is comprehensive and commensurate with its need, good privacy practices are part of the agency's privacy culture, and planning / implementing the privacy work programme and other activities are strategic and appropriately resourced.

211 PMAF self-assessments focus on leadership and privacy activities, policies and frameworks, rather than in-practice outcomes. However, an agency inevitably must use its real-world performance to inform its assessment and plan for any frameworks it needs to implement to achieve higher ratings. The purpose of PMAF reports are redundant if an agency considers itself at the 'managed' end of the scale merely because it has privacy policies in place. A 'managed' rating is considered to be the target level of privacy maturity for most agencies.

212 Oranga Tamariki provided us with its PMAF reports for 2021, 2022 and 2023 as part of this review. These reports provide a helpful snapshot of how the organisation rates its own privacy performance and maturity levels from one year to the next.

PMAF report for 2021

213 In 2021, Oranga Tamariki rated itself as 'basic' in 23 of the 41 sub-criteria. It considered that it was at a lower 'informal' level for 7 of the sub-criteria, including privacy training, identifying Māori privacy interests, privacy and assurance and planning / reporting. However, it considered it was at a higher 'managed' level for 11 of the sub-criteria such as implementing privacy practices, having policies, knowing the agency's risks, and being transparent.

214 In the 2021 PMAF, Oranga Tamariki reflected that leadership messaging regarding privacy reinforces its importance, though messaging is not always consistent. While there was currently no scheduled regular engagement and oversight or periodic assessment of privacy culture, Oranga Tamariki said it had planned assurance activity and reporting in the pipeline.

215 Further, in 2021, frontline operative teams were provided regular communications from leadership regarding the agency's privacy values. At a National Office level, senior and privacy leaders regularly and consistently communicated what the agency's aims should be with regard protecting privacy, although Oranga Tamariki recognised that this was ad-hoc and engagement based.

216 Oranga Tamariki also reflected that given the sensitivity of information it works with, privacy awareness is strong, but is sometimes considered to be the responsibility of a few managers and specialists. Another comment stated that while Oranga Tamariki recognised it gave itself a 'managed' rating, it was aware that incorporation of good practices in core processes is not entirely consistent across all functions.

217 Overall, the 2021 PMAF report was a fair self-assessment of the agency's privacy maturity. However, it contained some over-statements, such as reporting that Oranga Tamariki is 'very strong as an organisation with respect to privacy given who and what it involves, respecting mana and integrity'.

218 In 2021, Oranga Tamariki notified seven privacy breaches to the OPC (noting that the legal requirement to notify only came into force part way through 2021).

PMAF report for 2022

219 In 2022, Oranga Tamariki notified 13 privacy breaches, a level we consider consistent with 2021.

220 The 2022 PMAF report included a statement from the Chief Executive which said 'this year we have significantly improved both kaimahi understanding and consciousness of privacy, and the process for the provision of information to adults who have been in care.'

221 In 2022, Oranga Tamariki ranked itself as 'foundational' in 15 of the sub-criteria.[42] It rated itself as 'managed' for the remaining 27 sub-criteria and did not rate itself as 'informal' for any of the sub-criteria. As in 2021 it noted that 'incorporation of good practices in core processes is not necessarily consistent across all functions'. A 'managed' ranking (the highest level) is inconsistent with this observation.

222 The agency also noted the expectation to 'be a capable Treaty partner by supporting the Crown to fulfil its stewardship responsibility and strengthen Crown's relationships with Māori'. To this end, Oranga Tamariki said that its 'organisational values reflect our aspirational goals and given these, and our responsibilities under the Oranga Tamariki Act, we believe it is right to set ourselves a higher obligation as a target. While we believe we could easily be considered 'managed' by another agency's measure, this higher standard we aspire to means we consider a 'foundational' rating more appropriate.' Clearly, Oranga Tamariki thought it was doing well when it came to the identification of Māori privacy interests, and indeed, better than most other ministries.

PMAF report for 2023

223 In 2023, Oranga Tamariki notified 13 privacy breaches. This represents an unchanged figure from the previous year's figures.

224 In 2023, the PMAF report included the following comments:

[42] Noting that the sub-criteria increased from 41 to 42 in 2022.

> *Although we assessed our privacy maturity at a 'managed' rating for most elements in our 2022 report, work continues to seek improvement where we can, and for the 2022-2023 financial year we have identified improvements allowing us to rate ourselves as 'managed' for two additional categories, privacy training and identifying Māori privacy interests.*
>
> *Oranga Tamariki strives to go above and beyond legislative requirements to ensure respectful management and use of information, particularly information that is considered taonga, and the mana of all affected persons and is therefore pleased to report that it has achieved a managed rating in most categories of assessment.*

225 Oranga Tamariki scored itself as 'foundational' for only 13 of the 42 sub-criteria. It ranked itself as 'managed' for 29 of the sub-criteria. Again, it did not rate itself as 'informal' for any of the sub-criteria.

226 The 2023 report reflected that a key focus for 2023-24 was to analyse reported privacy incidents to identify trends, address root causes, and reduce frequency of reoccurrence.

227 The report from the Government Chief Privacy Officer in response to the 2023 PMAF assessment stated that 'the Ministry's stated achievements have largely focused on training, rather than broader aspects of leadership. It is clear though that there is a broad awareness of privacy responsibilities across the Ministry'. Given the Government Chief Privacy Officer was relying on the self-assessment of Oranga Tamariki to complete their report, the accuracy of their findings will naturally be limited by the reliability of those self-reflections.

Reflections on Oranga Tamariki's self-assessments

228 Since the first 2021 assessment, Oranga Tamariki reported that it has improved its privacy practices. However, since 2021 the same issues are identified as areas of concern, namely inconsistency across the agency and a failure to decrease the number of notified breaches.[43]

229 The agency repeatedly expressed ambitious goals for improving its privacy culture, and since 2022 has never ranked any of its activities at the lowest level 'informal'.

230 We consider the self-assessment of Oranga Tamariki to be generous. Without proper reporting processes and systems and while the overall privacy culture remains immature it is difficult for Oranga Tamariki to accurately assess what it does, how well it does it and how it might best target initiatives to improve.

[43] We acknowledge that an increasing number of notified breaches can, in some circumstances, reflect an improvement in privacy practices, in the sense that it reflects a better understanding of what constitutes a breach and a more transparent manner of dealing with breaches.

Oranga Tamariki staff perceptions

231 Kaimahi interviewed for this report were frank in their appraisals of processes and culture at Oranga Tamariki. Across a range of roles and locations, kaimahi spoke of the challenges inherent in the work they do and the commitment they had to making a difference. But they also offered some critical insights into the organisation and its culture. Taken together, they provide a valuable insight into how much work will be required to improve the privacy culture at Oranga Tamariki.

232 We provide short extracts below in an anonymised form. Each one is a verbatim quote from a staff member.

On the overall privacy culture at Oranga Tamariki

- It's not taken seriously enough.
- It's a very complex environment to be thinking about privacy and there's so many competing interests, child, family members.
- I don't think there's good consistent understanding of the Privacy Act.
- The social workers at each site are really good social workers. They are not technology people. They're not privacy people.
- The agency as a whole is quite immature in what you call back office functions; privacy, information management, information security, physical and protective security. They are not as strong as they should be, and I think it is because it is a social work agency. It's not an enforcement agency, so that recognition of rules and regulations around our data and our information probably aren't as stringent.
- The only time they [staff] probably give genuine 100% attendance [to privacy] is through trainings and refreshers and updates like that and then it is just through a single review.
- People at the front line are very confused. They get messages around section 66C which wants to encourage broader sharing of information so that we make sure that we keep people safe and then the messages from privacy border on fire and brimstone about the breaches. They don't know what to do.
- Most of it is at the front-line and social workers are being asked to be so many different things and to really get them to understand the complexities of information sharing as well as training them to actually do the job and the fact that they have got caseloads that are through the roof and we have got vacancies everywhere.

On access to personal information

- There is quite a bit of information that is sent around internally that has quite a bit of personal details and I don't see anything that is password protected. There is quite a lot of detailed personal information that is shared amongst people internally that potentially doesn't always need to be shared.

- There is a real tension about how much information we share with our partners. I know there is a view from some social workers and from some of our contracted partners that too much is shared in the referral form and then probably half the people think that we don't provide enough information for our partners to understand about the young person's trauma.

- People didn't think that social workers or others would be doing what they're doing, but also that you should only really be looking at your own cases. You know some of those hard line messages, you know this is the expectation. When you get CYRAS, and who's got CYRAS and why they've got CYRAS

On reporting privacy breaches

- Not all the privacy breaches have been reported.
- If [a breach] is not flagged with the Privacy Team, it's not really clear what happens.
- A couple of months ago someone told me what had happened and I was like 'have you consulted with the Privacy Team, it looks like this might be a privacy breach?' and they just hadn't turned their mind to it at all.
- We are inconsistent with how we deal with these (breaches).
- Our philosophy with breaches is that generally we don't let the person know that they have breached. There is a method in our madness because if we do their behavior will change (towards clients) and, you know, people don't do it on purpose.

On monitoring privacy

- There are some who believe checks like random checking for unauthorised browsing would not fit with the agency's culture which is educative rather than compliance and enforcement.
- Usually I would need to have an inkling that something wasn't quite right for me to then request a footprint or to go and do a bit more exploration.

On technology

- CYRAS is a dog. It's an antiquated system.
- At the moment CYRAS doesn't enable us, and it doesn't stop us doing certain things but a replacement might.
- Who's got CYRAS is a massive question and how do we make sure the right people have CYRAS and how do we make sure that when you move roles you've got the correct CYRAS access for your new role and it's not just what you had previously.
- I would say we have a mixed model where there is the potential to have two ways of capturing data. A paper file and an electronic one. We encourage obviously people to do things in the system and upload documents etc, etc as one source of truth. [But] when you receive something in its paper form you aren't to dispose of it. So, if you have received it in a paper form and you have then uploaded that into a system, you retain the paper document.
- There are laptops floating around with [third parties – identity withheld] because obviously we were trying to do prototype partnerships with them and none of this has been done with malice. But the organisation doesn't know enough about technology to do this. I know there's laptops floating around that are our laptops and lots of people probably have access to them. They've got a password. They could give it to the person sitting next to them.

On training

- We don't have a compliance team so we don't have people who are able to go look at those sites that say 11 out of 13 people haven't completed their privacy training. We could do it, we could dedicate time to do it.
- I just know people need reminders all the time because of our turnover and our busyness.
- Ideally it would be incredible to have every social worker go through some really solid information sharing training but we are not even training them on some of the social work skills that – you know training is a big issue.
- I am not convinced when (Caregiver Information System - CGIS) was rolled out that the training was as good as it could have been. There have been a number of examples with that system that people just don't understand where to save things, permissions etc.
- I think they are worried about privacy breaches and what could happen to them. I think everybody is more worried and I think the privacy modules have had – because it has been compulsory – I think it has opened people's mind up. I think some of the ways those modules are written are actually more about practice and we have been trying to work with the privacy team to say, 'Don't do an example of a technological breach because social workers won't understand it'.

On accountability

- We are in a world where compliance somehow has become a dirty word and yet that is actually what we are striving for most of all – we just don't like to say it. I am not a believer in that. I am a believer in compliance and so I find the push for a greater decentralisation troubling because I feel like you lose oversight. It makes the challenges that we have even greater.
- We are not operating under a zero tolerance policy. In fact the opposite to that.
- We need better top down messaging from leadership. That is where we are missing.
- if you have the head space and, you know, impetus to do that, some people will but again that busyness at the front line, all the stuff that people are dealing with that's really hard to find that head space and if you also don't have practice leaders and supervisors who can also build that space cause they're just as busy as well, that's really hard to find that head space. If you also don't have practice leaders and supervisors who can also build that space because they're just as busy as well you know that all kind of compounds. We have practice leaders who still don't understand information sharing legislation and we're four years in and they're leaders of practice on their sites and they can't speak to information sharing. They still don't understand it, some of them. So I think that's an indication of everything is just so much and how do we upskill our leaders to be able to lead that kind of way as well because they haven't experienced it because they've often come, been a social worker, they've just kind of stepped up. They haven't had that experience either, so that's a real issue for us is that everything is just piecemeal and reactive.

On taking personal responsibility for privacy

- I have too many things on my plate to think about privacy when it's not in my portfolio at the moment unfortunately.
- Sometimes whiteboards would be used and there are reminders that come out quite regularly making sure desks are left clean and files are put away but, being totally honest, in the busyness sometimes…
- A lot of it is common sense but then when you are out there in it and you are working alongside whānau who are nervous and have hurt - that's when it becomes a little bit grey and a little bit tricky.
- One of our experienced [role withheld] emailed a couple of days ago saying, 'I didn't realise health education assessments were confidential to whānau and clients'.
- Privacy is obviously a massive thing but when you are dealing with kids in custody and placements and really stuff that is in the now you forget about those sorts of things sometimes.
- You need the head space to go, 'Actually privacy isn't an add on, it's a fundamental part of everything I do in the same way that the way I attract the whanau is fundamental to how I practice social working'.

What does good privacy practice look like for Oranga Tamariki?

233 A starting point for considering what constitutes ‘good’ privacy practice is to address compliance with the legal requirements applicable to the collection, use, disclosure and storage of personal information, and the associated obligations that apply to that information under the Privacy Act 2020. This is addressed above, at paragraphs 49 to 95.

234 However, good privacy practice requires much more than compliance with the law. The kaimahi who deal with privacy compliance issues are often required to make numerous judgment calls and difficult decisions, in the face of legal tests which include elements of subjectivity and other nuances which make a definitively ‘correct’ approach a rarity.

The importance of privacy culture

235 Good privacy practice needs to incorporate a framework, or ‘scaffolding’, within which the kaimahi who actually make the decisions necessary to operate are sufficiently supported and empowered to make the best decisions from a privacy perspective. This framework should take into account the operational and other constraints with which kaimahi are faced and the circumstances in which a decision is made.

236 In order to create such a framework, an organisation needs to develop a culture whereby privacy is enmeshed in each aspect of its operations. This involves adopting a privacy-centric approach, with processes and systems designed with privacy considerations in mind, and organisational measures implemented to mitigate the risk of not just significant privacy breaches, but also systemic misuse of personal information.

237 In the case of Oranga Tamariki, good privacy practice requires the promotion of a privacy-centric culture, and systems and processes to underpin that culture, which acknowledges the status of all personal information as taonga. This is currently lacking.

238 Oranga Tamariki has a statutory obligation to have, as its first and paramount consideration, the well-being and best interests of the child or young person.[44] Oranga Tamariki will fail to deliver on this statutory obligation if it cannot properly manage the personal information of children, young people and whānau, as that personal information is an integral part of the child/young person’s well-being and best interests.

239 Part of developing a culture of privacy recognises that the success of Oranga Tamariki to an extent depends on the establishment of trust with the children, young persons, and their whanau with whom Oranga Tamariki engage. That trust is rapidly eroded on each and every occasion which personal information is misused and otherwise not treated with the respect that it deserves. One staff member interviewed as part of this review put it well:

> *All the data that we hold in [Oranga Tamariki] for a young person – it is pivotal and also it can ruin their lives.*

Putting privacy into practice

240 It is essential for each individual involved within the organisation to treat privacy as an integral part of what they do and how they do it. In the absence of proper consideration of privacy implications in its day-to-day operations, Oranga Tamariki simply cannot deliver on its most critical mission to put first the well-being of children and young people. Privacy cannot be simply an afterthought.

[44] Oranga Tamariki Act 1989, section 4A.

241 In an ideal world, an organisation develops processes and procedures which incorporate privacy by design and does so from inception. This helps the organisation to embed the technical and organisational measures which allow it to operate in a manner which is inherently privacy-compliant.

242 However, where the processes and procedures used by an organisation are inherited from another organisation (in the case of Oranga Tamariki, as a consequence of the separation from the Ministry of Social Development) and / or evolve over a period of time during which privacy is not a primary consideration, some backfilling is required. That backfilling can take time, since systems (especially those relying on complex and expensive technology) will likely require redesigning to incorporate more privacy-centric measures, yet may only receive the necessary attention as and when budgets permit.

243 The absence of robust, privacy-focused systems (especially technology systems) should not act as an inhibitor of privacy compliance. While the journey towards best practice may be slower, an organisation which adopts a positive privacy culture can face privacy challenges head-on, and is better-placed to design and implement new systems when the opportunity arises.

244 A positive privacy culture should be supported by specific practical measures. To start, as systems and processes are introduced, they should be designed with privacy in mind, adopting concepts of ‘privacy by design’. This means that privacy controls should be incorporated as an inherent feature of systems and processes, and systems and processes which do not support privacy controls should be earmarked for review and replacement or revision.

245 It is key to involve privacy advisors at the early stages of systems and process design, with privacy a key consideration. This allows for technical measures (IT security, physical controls) to be implemented alongside organisational measures (instructions, policies, procedures), with the importance of both emphasised.

246 Further, a proactive programme of remedial activities should be adopted, incorporating a clear roadmap which sets out the organisation’s journey towards ‘better’ compliance. This involves checking that contracts and other arrangements with third parties include appropriate protections and safeguards relating to data management and privacy, and relationships with key stakeholders with whom personal information is shared should be the subject of regular oversight. We understand that while this is not the case currently, a review of the arrangements with external parties is underway. In the future, other remedial activities requires the privacy function to be well-resourced, to a degree commensurate with the importance of privacy to the organisation.

Collection of information

247 Under the Privacy Act, personal information should only be collected for a specific purpose, and should only be collected where necessary for that purpose. Specifically, personal information should not be collected ‘for the sake of it’ or ‘because it can be’, and instead should only be collected where such collection is necessary for a defined purpose. Forms, processes, and systems should be designed to only capture the necessary information and mitigate the risk of overcollection.

248 The purposes for which personal information can be used should be clearly stated and understood by all kaimahi who collect and use that information. This means that:

a accessible policies should exist and be readily available to provide guidance regarding the use of personal information other than for the purposes for which the information was collected, with appropriate escalation procedures to facilitate the delivery of specialist guidance where difficult decisions need to be made; and

b technical controls and other organisational measures should be in place to mitigate the risk of use of personal information for unauthorised purposes.

User-friendly policies and guidance

249 Privacy policies, guidance and processes need to be accessible to those who deal with difficult privacy decisions on a daily basis, and give kaimahi the confidence needed to be able to make tough calls with accuracy. Specifically:

a guidance should take into account the operational challenges that kaimahi face and include practical recommendations about what to do when faced with actual, real-life operational situations;

b operational procedures should recognise and take into account the technical limitations that Oranga Tamariki faces and provide guidance on appropriate responses to those limitations;

c decision trees should be easy to follow and access, to facilitate kaimahi making decisions without needing to exercise significant levels of individual discretion (in other words, appropriate 'scaffolding' to direct kaimahi to make the best decision in the circumstances), with an appropriate support framework in place for more difficult decisions to be made quickly with the support of others within Oranga Tamariki;

d practical training should be made available, which should be tailored for Oranga Tamariki and should align with the organisation's values and tie in with the organisation's critical mission; and

e certainty should be included in policies regarding disciplinary action for deliberate or particularly serious breaches compared to an educative focus and support for kaimahi in the event of a privacy breach more generally. This will give kaimahi the confidence to report privacy breaches when they occur, rather than withholding incidents out of fear of the consequences.

250 Stakeholders (including kaimahi, tamariki and their whanau) should be made aware of how the organisation uses personal information and why, using language that is easy to understand and does not seek to over-explain. All stakeholders should be made aware of their rights and responsibilities with respect to personal information, and what they need to do to exercise those rights.

251 Additionally, operating procedures should emphasise the importance of the privacy controls that are embedded within systems and processes, with reference to the critical mission of Oranga Tamariki, so as to discourage the use of workarounds (such as the creation of unnecessary documents containing personal information).

252 Guidance, systems and processes should work to empower kaimahi to make difficult decisions quickly, based on the information available to them. Policies and guidance should also acknowledge that difficult decisions and line calls will need be made – often in the field – which may require a delicate balancing exercise, and/or the support of specialist advice.

253 Further, supporting rationale for systems and processes should be well documented, which means completing PIAs when new systems and processes are introduced and monitoring the implementation of controls from previous PIAs. Records of key decisions should also be retained and available for audit.

254 Oranga Tamariki should also ensure that it engages with Māori stakeholders to confirm that systems and processes are aligned with the concepts of mana and tikanga.

Retention

255 As required by the Privacy Act, personal information should only be retained for so long as is necessary for the purposes for which it was collected. This means that information should be securely destroyed when it is no longer required to be retained, with clear instructions to kaimahi regarding how that information is to be destroyed, and when. In order to enable an effective

information retention system, processes should be designed to automatically apply retention periods to defined categories of information in a manner that is consistent and easy to understand.

Accountability

256 Accountability in a legal sense (rather than personal accountability for breaches) requires processes in place to manage compliance. In essence, accountability means that:

a stakeholders should be able to exercise their rights, including statutory rights of access, in a consistent and timely manner;

b privacy breaches should be promptly identified and documented;

c a clear plan should be in place for responding to privacy breaches, with appropriate levels of escalation and appropriate external advisors on hand to lend expertise when required;

d privacy breaches should be notified to the Privacy Commissioner and affected individuals when required by law;

e root causes of privacy breaches should be identified, and systems and processes improved to take into account shortcomings and mitigate risk of repeat breaches;

f privacy breaches should be accepted as likely to occur (especially given the challenging environment in which kaimahi operate), but the organisation should commit to learning from its experiences, and should be open about the challenges it faces to comply;

g kaimahi are encouraged to report privacy breaches and ‘near misses’ when they occur;

h the organisation should engage frequently and constructively with the Privacy Commissioner, to identify areas of focus and learn best practice; and

i the organisation should accurately use established tools (such as the PMAF tool) to monitor maturity levels and progress.

Recommended action points

257 As discussed above at paragraph 43, a table of recommended action points for Oranga Tamariki following this review is included below. We also recommend sharing this report with the OPC and the Children’s Monitor. Both have an interest in ensuring Oranga Tamariki makes progress.

258 To ensure progress is made against these action points we recommend the senior leadership team conduct a further review in 12 months’ time.

Area	Action point
Workplace practice	• Restrict open access to information by applying technological controls such as confidential file locks and graduated access to individual files. • Limit the amount of personal information shared amongst kaimahi unnecessarily. Information should be shared on a ‘need to know’ basis only, even internally. • Develop guidance on practical ways to manage documents, share information in group settings and maintain confidentiality. • Upskill kaimahi in basic computer skills and encourage all staff to use digital records in preference to paper. • Increase the resourcing of the privacy team.
Accountability and performance tracking	• Encourage reporting of near-misses and all privacy breaches. • Introduce transparent privacy targets. • Implement leadership for privacy, including clear lines of accountability and ownership, including responsibility for compliance. • Drive a prevention first approach by introducing quarterly reporting to the Chief Executive and senior leadership team of a range of identifiable outcomes. These could include: ○ the number of notified breaches; ○ the number of other breaches; ○ the number of reported near misses; ○ the number of privacy complaints registered with Oranga Tamariki; ○ the time taken to respond to a request made under the Privacy Act for personal information; and ○ reports on random checks for employee browsing and spot site visits to check on document and information management. • Move the privacy team to a more central location in the agency to better align delivery and performance. • Elevate the Privacy Officer role to signal to all kaimahi the importance of privacy and compliance with the Privacy Act. • Conduct monitoring of access to personal information to pick up on unauthorised access and employee browsing and spot site visits to check on document and information management.

Area	Action point
	• Ensure PMAF reporting tools are accurately used to monitor maturity levels and progress. • Ensure that contractual arrangements with external parties provide for explicit requirements and responsibilities for data management and privacy.
Training and policies	• Develop and implement training that is practical and aimed at the day-to-day situations kaimahi face. • Consider replacing online privacy module with face-to-face training. • Streamline privacy policies and guidance. Make sure they are published in an accessible location for kaimahi. • Weave privacy into the education programme for front-line kaimahi. • Encourage Oranga Tamariki kaimahi to see obligations under both Oranga Tamariki Act and Privacy Act as aligned. Guidance, systems and processes should work to empower kaimahi to make difficult decisions quickly, based on the information available to them. • Acknowledge in policies and guidance that difficult decisions and line calls will need be made which may require a delicate balancing exercise and additional support. • Ensure that disciplinary processes for privacy breaches are clearly understood and consistently applied across the organisation. • Certainty should be included in policies regarding disciplinary action for deliberate or particularly serious breaches compared to an educative focus and support for kaimahi in the event of a privacy breach more generally.
Systems	• Ensure that technological upgrades (including for CYRAS) are designed to incorporate privacy-centric measures. • Privacy controls should be incorporated as an inherent feature of systems and processes, and systems and processes which do not support privacy controls should be earmarked for review and replacement or revision. • Engage with Māori stakeholders to confirm that systems and processes are aligned with the concepts of mana and tikanga. • Check that contracts and other arrangements with third parties include appropriate protections and safeguards, and relationships with key stakeholders with whom personal information is shared should be the subject of regular oversight. • Processes should be designed to automatically apply retention periods to defined categories of information in a manner that is consistent and easy to understand.

Appendix A: Table of policies, guidelines and trainings review

Title of the policy/guideline	Brief summary of the policy/guideline	What part of the Privacy Act it relates to
Privacy Guidelines	Supplements the OT Privacy Policy which sets out the standards for the Ministry based on those principles and other responsibilities under the Privacy Act, Te Tiriti o Waitangi, and Section 7AA of the Oranga Tamariki Act 1989 to ensure we treat the personal information we hold lawfully, respectfully, and with care. *Scope* • The Privacy Policy applies to all permanent, fixed term, temporary, seconded, and casual employees, contractors, consultants, and volunteers, independent members of Oranga Tamariki committees and boards, and external parties who have a contractual relationship with Oranga Tamariki (e.g., service providers, partners, and certain NGOs). *Examples of PI held by OT* • Information about tamariki, rangatahi, and their whānau, others who may have a role in the care of a child, or individuals who raise reports of concern, e.g., names and contact information, details of involvement with Oranga Tamariki (through notes, recordings, correspondence, or administrative records like expense reports), health information, criminal records, allegations or evidence of neglect or abuse, photographs or letters, and family histories. • Employee and contractor information, e.g., names and contact information, demographic information, job applications, immigration status, vetting checks, remuneration details, employment history, health information, performance assessments, and disciplinary records. *Other considerations* • Treaty of Waitangi and Māori Data Soverignty ○ It is important that Māori Data Sovereignty and other obligations under Te Tiriti of Waitangi and Section 7AA of the Oranga Tamariki Act are considered alongside the principles of the Privacy Act. • Factors to take into account may include: ○ whether the personal information collected or held by Oranga Tamariki ‘may be considered taonga’; ○ whether the use of the information is appropriate in light of, or necessary to support, our treaty obligations; ○ whether retention of personal information may be necessary to preserve the whakapapa or any individual or group; and ○ whether the information is or will be easily accessible to those the information is about or those who may have interest in the information, including hapū, iwi, and whānau.	IPP 1 - 11
Data Protection and Use Policy	DPUP guides social sector agencies in the values and behaviours that underpin the respectful and transparent use of data. The DPUP is not legislation but uses the PA and the IPP’s as a base to build best practice in information and data management. Four key guidelines:	IPP 3, 4, 6, 7, 10 Section 201 Part 6

1. Purpose Matters – It's important that we only collect and use personal information for distinct and clearly-defined purposes. Personal information should not be collected otherwise, for example ‘just in case’ it might be useful for something in the future.
2. Transparency and Choice – We should also ensure people are informed as much as possible about what personal information we hold about them, how we are using it or sharing it, and what choices they have in regard to our handling of their personal information.
3. Access to Information – People have a right to ask us for access to their personal information or ask us to correct personal information we hold that they believe is inaccurate. They must be made aware of these rights, have processes available to them that are easily understood and followed, and access (or correction) should be provided within a reasonable timeframe. Consideration should be given to different access needs, e.g., in respect of children, people with low vision or intellectual disabilities, or people with low English literacy.
4. Sharing value – Oranga Tamariki already understands the necessity of partnering with a range of other groups, agencies, and organisations to realise oranga tamariki. This principle emphasizes the importance of working together and sharing information for better insights and outcomes for tamariki and their communities.

Privacy Incidents

- Reported to the OT Privacy Team who decide whether it is a notifiable breach that needs to be escalated to the OPC
- Privacy near misses should also be reported
- Privacy incidents managed in accordance with the OT Privacy Incident Process
    - Under this process the Privacy Team will perform an initial assessment, evaluate the risks, and provide guidance and support to help the relevant team contain the incident, address any risk or harm, progress any investigation, and design remedial actions where appropriate.
- All employees and partners/agents must escalate incidents of actual or potential privacy incidents immediately once they are identified. Escalation will generally involve notification of one’s manager and the Privacy Team. Failure to do so may result in disciplinary action, depending on the particular circumstances.

Third party providers

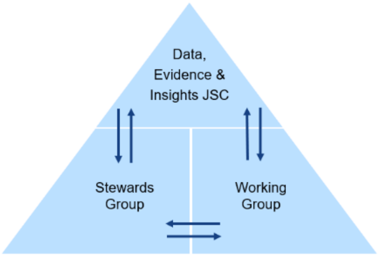
- Sets out the Privacy Act framework whereby agencies will be held accountable for personal information held by third party providers acting on their behalf.
- Relationship managers should ensure they are aware of these obligations and satisfy themselves that the provider has appropriate policies, processes, and controls in place, including appropriate reporting mechanisms. A Privacy Impact Assessment will generally be required for any such engagement with a third party to review and address these privacy considerations.

Privacy Impact Assessments

- Each time a process or system that collects, uses, and/or stores personal information is reviewed, changed, adopted or developed (including the engagement of a third party provider), the Privacy Team must be engaged to determine whether a Privacy Impact Assessment (PIA) is required.
- Where there is likely to be a public interest, we will aim to publish either a summary of the PIA or the PIA itself on our website.

	Research Purposes • Sets out that OT may holds personal information that was obtained in connection with one purpose to use the information for another purpose if the agency believes, on reasonable grounds, that the information will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned. • Likewise, where OT releases information for research or statistical purposes, unless a legitimate research request requires otherwise, the information should be released in a form that does not enable the identification of an individual. *Overlap with OIA* • As a rule of thumb, the OIA is premised on the disclosure of information unless one of the grounds for withholding exists. However, the Privacy Act is premised on the non-disclosure of personal information (about someone other than the requester) unless an exception applies.	
Managing privacy incidents	Sets out: • What a privacy incident is • What you should so if you suspect a privacy breach • Four step privacy incident process: contain, evaluate, notify, prevent • Contains the link to the Privacy Incident Report template to be sent to the Privacy Team.	Part 6
Managing personal information	Sets out: • What personal information is • Principles of personal information management: ○ Information Privacy Principles ○ Principles of Māori Data sovereignty ○ Data Protection and Use Policy (DPUP)	IPP’s 1-13
Managing electronic records	• States that information created or received by a government organisation in the course of busienss is a public record, whatever format it comes in. • States that this is a ‘business decision to be made based on the message channel being used and the context of the message. • *Maintaining and storing* ○ All records must be kept for as long as required until they can be disposed of under the Public Records Act 2005 and the Contract and Commercial Law Act 2017. ○ Electronic records should be stored once in the appropriate business system, that supports the related function or activity e.g: ▪ Emails including attachments, relating to a case file should be uploaded into CYRAS ▪ OneDrive business content, should be moved into SharePoint ▪ Call recordings (with or without transcript) should be moved into SharePoint	IPP 5 OIA PRA 2005 CCLA 2017

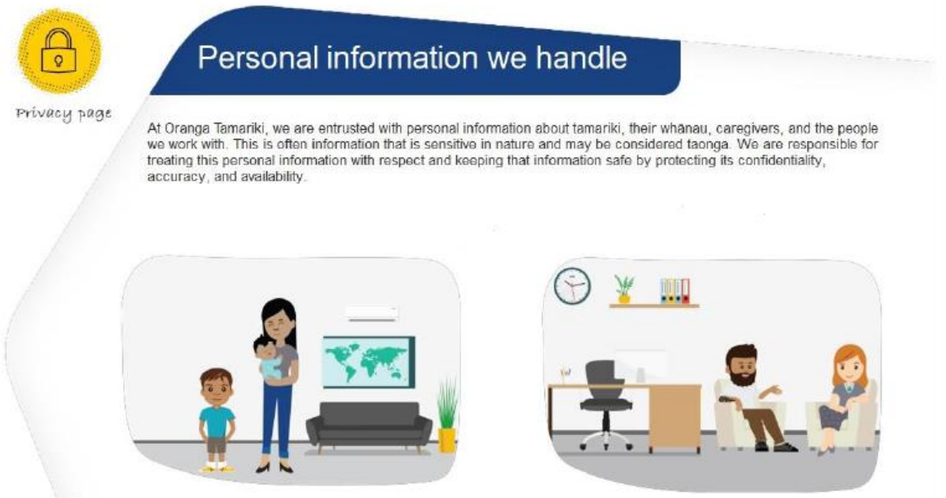
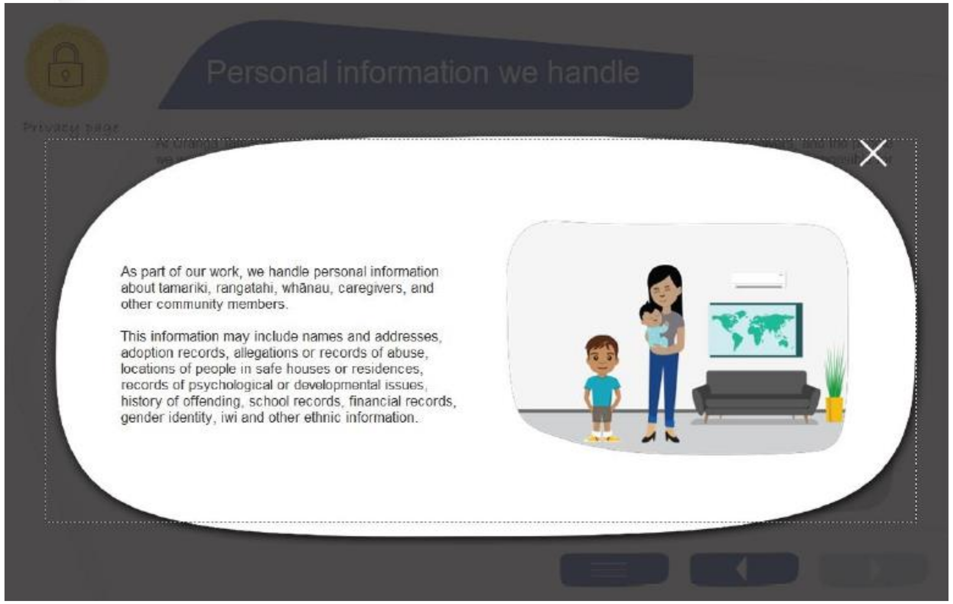
	• To meet our legislative obligations, we must protect our records from unauthorised or illegal access, loss, deletion and destruction. It is everyone's responsibility to safeguard our information.	
Information security	This document outlines the fact that information security is everyones responsibility. To protect information from unauthorised or unlawful access, alteration, loss, deletion, and/or destruction, it suggests: • You must secure all information (both electronic and physical) in your workspace. This includes: ○ at the end of the work day ○ when away from your workspace for an extended period ○ when working from home. • Lock (or log out/shut down) your devices when you are away from them. • Lock away mass storage devices such as CD, DVD, USB drives, or external hard drives when not in use. • Keep your paper files secure. • Treat all information related to your role as confidential (whether about colleagues or clients). This document includes information on what and where to record information security interests such as an unauthorised system access, lost or stolen devices, suspicious emails, lost or stolen records, and failed delivery of Iron Mountain files. Steps to be taken include: 1. Contacting the Service Desk to report an incident 2. Informing your manager and emailing the Information Management Team. It also provides information of reporting any security concerns or near misses, and provides access to a 'raising concern page' for more information on reporting issues while maintaining appropriate confidentiality and respecting others' privacy. *Security classifications* Oranga Tamariki are required to mark information for appropriate protection and management by the NZ Protective Security Requirments (PSR), and use Microsoft AIP (Azure Information Protection) to do so. The classifications include: unclassified, in confidence, and senstitive. The document sets out the thresholds for each classification.	IPP 6 Part 6
Identifying and preventing privacy incidents	Sets out what a privacy incident is – any situation where someone's privacy has been interferred with, typically through the unauthorised or inadvertent disclosure of their personal information, and explains that a privacy incident can involve a breach of any of the principles found in the Privacy Act. It describes 'near misses' as an incident that could have resulted in a privacy breach but did not – e.g. an envelop left on the wrong desk but retrieved before its opened. *Report early, report often* This states that privacy incidents do occassionally happen, and that OT takes a 'no blame' approach to incidents caused by inadvertent employee error. Steps to be followed are: 1. Notify your manager of all privacy incidents and near-misses as soon as possible. 2. Report privacy incidents to the Privacy Team.	Part 6

Data Governance Structure: Proposed Structure	Recognises that the organisation's approach to data governance needs to be holistic in nature, ensuring not only that staff at a particular level derive benefit from it, but also that those same staff are equipped to govern data in conjunction with and in support of those operating at other levels.  Data, Evidence & Insights JSC Stewards Group Working Group On the basis of this holistic approach, data governance needs to bring together the top-down focus and an operational and bottom-up perspective. The recommended structure has three, interrelated elements: 1. Data, Evidence and Insights JSC (active/established): The JSC aims to support the Sponsors and Senior Responsible Owners (SROs) by providing overall direction, including ensuring that our understanding of how tamariki are experiencing care is current, accurate, and equitable. a. Approve: Data governance roles, data principles, enterprise data model, metadata structure, data access and permissions, business processes, code structure and maintenance, peer review process, data governance approach and establishment, budgets and finances, projects. b. Can direct: Data Stewards Group and Data Governance Working Group. 2. Data Governance Working Group: The group is responsible for the establishment of data governance on behalf of the Data, Evidence and Insights Joint Steering Committee (DEIJSC). The group reports to DEIJSC and will advise the DEIJSC on high level and policy matters and have delegation to make some lower-level decisions. The group also provides the strategic direction on the organisation's governance of data and information. a. Approve: Matters as escalated by DSG, D&I communication and engagement, information and data storage practices, data management foundational practices and processes. 3. Data Stewards Group: The DSG brings together data stewards from different workstreams to advise and make decisions on tactical matters. The group consists of data stewards from a wide range of business units of Oranga Tamariki. The group is responsible for the implementation of decisions within their business groups. The group reports to the Data Governance Working Group on Data Quality matters. a. Advice on: Data accessibility, permissions and storage, metadata structure and maintenance, business processes, code structure and maintenance, peer review process, inter-agency data sharing. Possible future capability: Inter-Agency Data Management Network	IPP 5, 11
Data Products Privacy Review Decision Trees	This document sets out how to determine if a privacy review is required in relation to Recreated Data Products and New Data Products.	IPP 10 and IPP 11
Evidence Centre Privacy Review Decision Tree	This document sets out how to determine if a privacy review is required.	IPP 1, IPP 10 Part 6

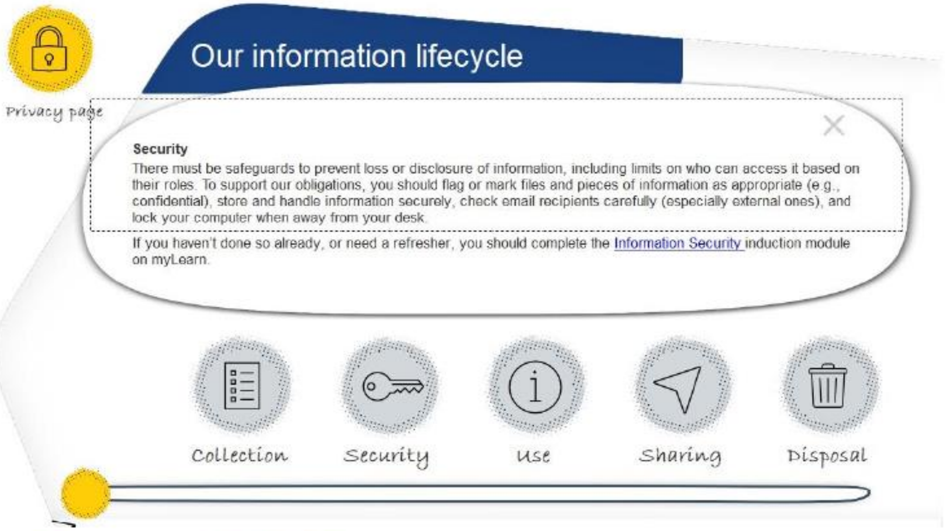
Principles of Māori Data Sovereignty	This Te Mana Raraunga Brief provides a general overview of key Māori Data Sovereignty terms and principles.	Various: IPPs 1,2,3,4,5,9,10,11
Questions to ask yourself when analysing information	Questions to ask when analysing a page: Does this page contain information relevant to the requestor's demand? • If NO, then remove the page in full. Does not require a code. • If YES, is there an actual risk of harm if we release this information? Identify the actual risk, such as risk: • of potential harm to a child? • of preventing a parent/caregiver using the service so there are fewer protective "eyes" on a child? • to someone's personal safety? • of preventing someone to make a notification again? • to a child's ability to disclose? • of damage to any relationship – personal, professional or community? • of intruding into another person's privacy in a way that is unwarranted in the circumstances? • of prejudicing the ability of Oranga Tamariki or the Police to conduct an investigation? • of other system conditions limiting our ability to release this information, e.g., legal privilege, court reports or FGC proceedings? • What action mitigates the risk? This could be redaction with explanation, writing of summary, seeking consent, getting more information to better your understanding. • Release the information after assessing and minimising the risk	IPP 10 and IPP 11
Records Management Policy	"Oranga Tamariki will continue to manage a programme of work to continually improve recordkeeping, recognising the current state of inherited records management practices. The programme of work will ensure that records are appropriately created, managed and disposed of in the course of business and according to the Public Records Act 2005 and Archives New Zealand's Information and Records Management Standard." <u>Specific records management requirements:</u> • Creation of Records: Records will be created in a manner that supports business processes and systems. Records should be full and accurate to the extent necessary to conduct our functions and processes. • Management and Storage of Records: The content, context and structure of records will be managed in line with records management procedures to facilitate information retrieval and re-use and ensure records are securely protected and not illegally disposed of. • Access to Records: Records will be maintained in an accessible form so as to be used for decision making, • accountability and reference in accordance with legislation and standards. • Disposal of Records: Records will be reviewed for their continuing value and disposed in accordance with an approved Disposal Authority.	IPP 5 and IPP 9
A Quick Tour of the Privacy Principles	Sets out all 13 IPPs under the Privacy Act.	IPP 1 – IPP 13

Oranga Tamariki Privacy Incident Process	Oranga Tamariki Privacy Incident Process: 1. Containment: It is important to act quickly to contain damage. The following actions may be appropriate: o trying to recover the lost or stolen information; o isolating or disabling a system that may be leaking information, or has been hacked; o stopping the practice that is causing the incident; o changing access codes or passwords; and o fixing any weaknesses in security. Any actions taken must be recorded in the Privacy Incident Register managed by the Information Management and Privacy team. The Information Management and Privacy team will decide who should be involved in management of the incident and if necessary, form an Incident Management Team. 2. Evaluation: Evaluate the incident to help you decide how to respond. This includes: establishing what personal information is involved, determining the cause of the incident and number of people who may be affected, consider what steps could be taken to prevent or lessen the likelihood of harm occurring. The impact on any employees should also be considered. 3. Notification: When determining whether the incident requires notification to the individual and/or the Privacy Commissioner, the following should be considered: o any examples of harm known to have occurred (such as financial impact, loss of opportunities, significant hurt or humiliation); o steps taken to contain the event and prevent harm from occurring; o how sensitive the information is from the affected individual's point of view; o how broadly the information has been shared and the recipient/audience; and o how likely it will be used to cause harm to the person and within what timeframes.	Part 6 of the Privacy Act
Privacy Impact Assessments	A Privacy Impact Assessment is a review and analysis of the privacy risks associated with a project or change process and, as the name suggests, an examination of the impact those risks may have on privacy. This document provides an outline of the utility of a PIA and the PIA process. The process involves a meeting with the Privacy Team to discuss the project, then safeguards and controls are put in place to eliminate identified privacy risks, then finally the template will be signed off.	
Oranga Tamariki Privacy Policy	This document sets out how Oranga Tamariki "ensure[s] that we treat the information we collect, hold, use and share, lawfully, respectfully and with care." Relevant policy statements include: • We will ensure that our handling of personal information complies with the 13 Information Privacy Principles (IPPs) set out in the Privacy Act 2020. The IPPs are considered to be the foundation of good privacy protocols.	IPP 1- IPP 13 Part 6

	• In applying these principles, we will ensure full consideration of our obligations under Te Tiriti o Waitangi and Section 7AA of the Oranga Tamariki Act. • We will promptly report privacy incidents resulting from unauthorised access to, collection, use, or disclosure of personal information to the Oranga Tamariki Privacy Team. The Team will also determine whether the incident needs to be reported to the OPC. • When reviewing, changing, adopting or developing new systems, processes, or services that collect, use, and/or store personal information (including the engagement of a third-party provider), we will consider potential privacy risks and engage with the Privacy Team. The document also sets out the key roles and responsibilities relating to the Policy. Measures of the success of this Policy are: • number of privacy incidents, including breaches notifiable to the OPC; • number and type of privacy complaints received; • training module completions; • number of Access directions, if any, received from the OPC; • number of Compliance notices, if any, received from the OPC; • Privacy Impact Assessments initiated; and • instances of advice sought from the Privacy Team	
Trainings		
Employee Browsing (Privacy at Oranga Tamariki) module	This module is intended to educate Oranga Tamariki employees about protecting and securing personal information from employee browsing. Employee browsing is searching, reviewing, or reading personal information we hold as an organisation without a legitimate business purpose (work-related). “A legitimate business purpose” means a valid reason for accessing, using, or disclosing personal information that is within the scope of your job responsibilities. The module goes through different scenarios and asks multiple choice questions which test an employee’s knowledge of what privacy breaches look like and the correct processes to follow. It then provides the correct answer and an explanation of the potential harms if an employee took the wrong approach.	IPP 5, 6, 10 Part 6
Data Privacy PowerPoint	An overview of privacy and personal information: definitions drawn from the OPC and the Privacy Act. How the Privacy Act speaks to responsibilities around personal information: explains the privacy principles and other statutes that can override the Privacy Act.	IPP 1, 6, 7, 12 Part 6
Privacy at Oranga Tamariki Module	The module intends to inform employees about four key areas: 1. What personal information is: definitions of privacy and personal information, for example:	Various: IPPs 1,2,3,4,5,9,10,11

	 Personal information we handle At Oranga Tamariki, we are entrusted with personal information about tamariki, their whānau, caregivers, and the people we work with. This is often information that is sensitive in nature and may be considered taonga. We are responsible for treating this personal information with respect and keeping that information safe by protecting its confidentiality, accuracy, and availability.  As part of our work, we handle personal information about tamariki, rangatahi, whānau, caregivers, and other community members. This information may include names and addresses, adoption records, allegations or records of abuse, locations of people in safe houses or residences, records of psychological or developmental issues, history of offending, school records, financial records, gender identity, iwi and other ethnic information.	

2. The information life cycle: States that the IPPs guide the way OT manages personal information in its life cycle of: collection, security, use, sharing, disposal. The module includes a slide on each element of the cycle, for example:

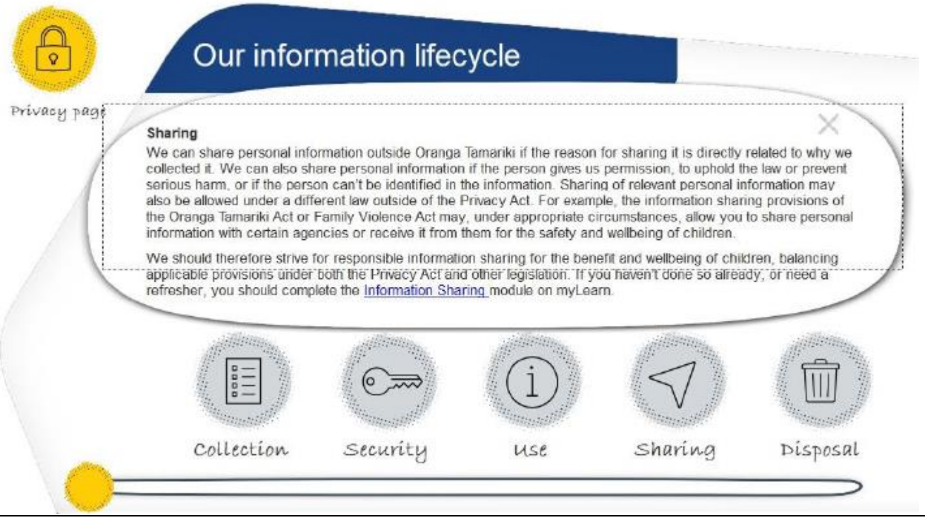


Our information lifecycle

Security

There must be safeguards to prevent loss or disclosure of information, including limits on who can access it based on their roles. To support our obligations, you should flag or mark files and pieces of information as appropriate (e.g., confidential), store and handle information securely, check email recipients carefully (especially external ones), and lock your computer when away from your desk.

If you haven't done so already, or need a refresher, you should complete the Information Security induction module on myLearn.

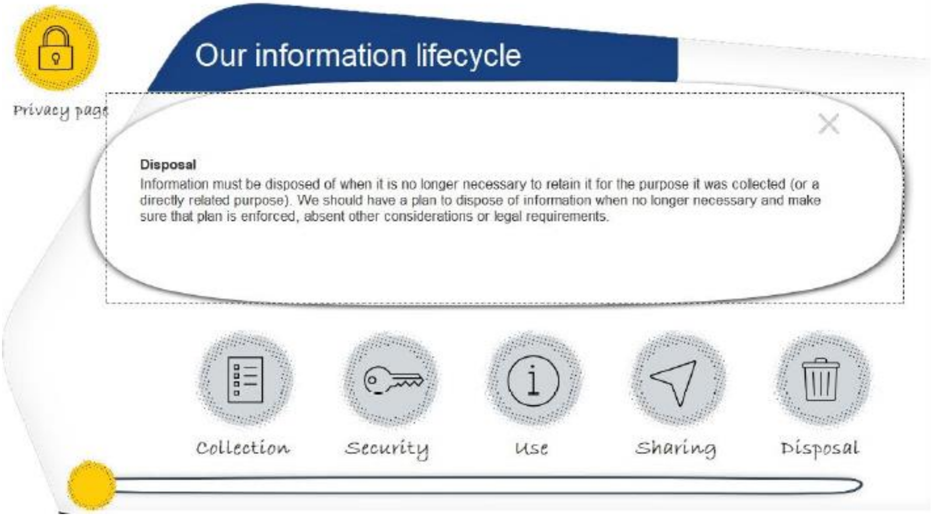


Our information lifecycle

Sharing

We can share personal information outside Oranga Tamariki if the reason for sharing it is directly related to why we collected it. We can also share personal information if the person gives us permission, to uphold the law or prevent serious harm, or if the person can't be identified in the information. Sharing of relevant personal information may also be allowed under a different law outside of the Privacy Act. For example, the information sharing provisions of the Oranga Tamariki Act or Family Violence Act may, under appropriate circumstances, allow you to share personal information with certain agencies or receive it from them for the safety and wellbeing of children.

We should therefore strive for responsible information sharing for the benefit and wellbeing of children, balancing applicable provisions under both the Privacy Act and other legislation. If you haven't done so already, or need a refresher, you should complete the Information Sharing module on myLearn.

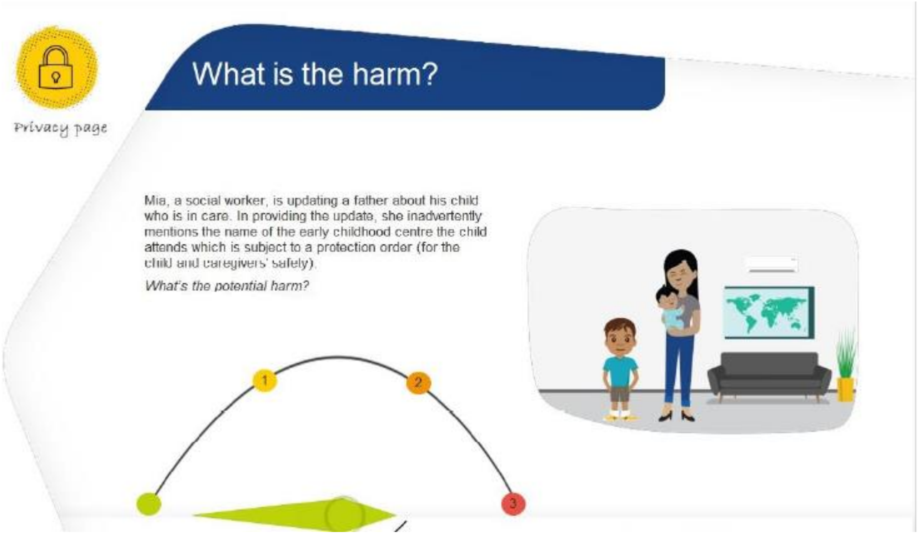


Our information lifecycle

Disposal

Information must be disposed of when it is no longer necessary to retain it for the purpose it was collected (or a directly related purpose). We should have a plan to dispose of information when no longer necessary and make sure that plan is enforced, absent other considerations or legal requirements.

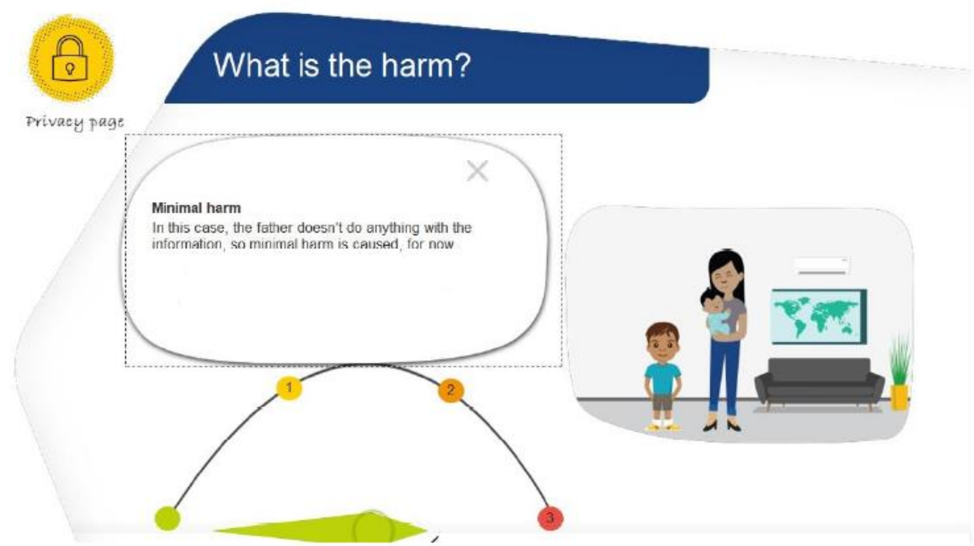
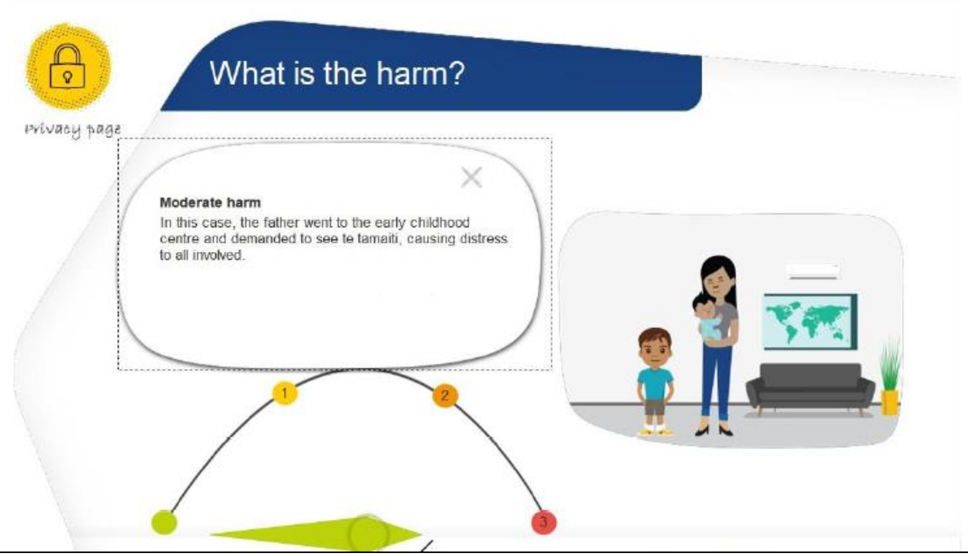
3. How privacy considerations should be woven into the work we do, for example:

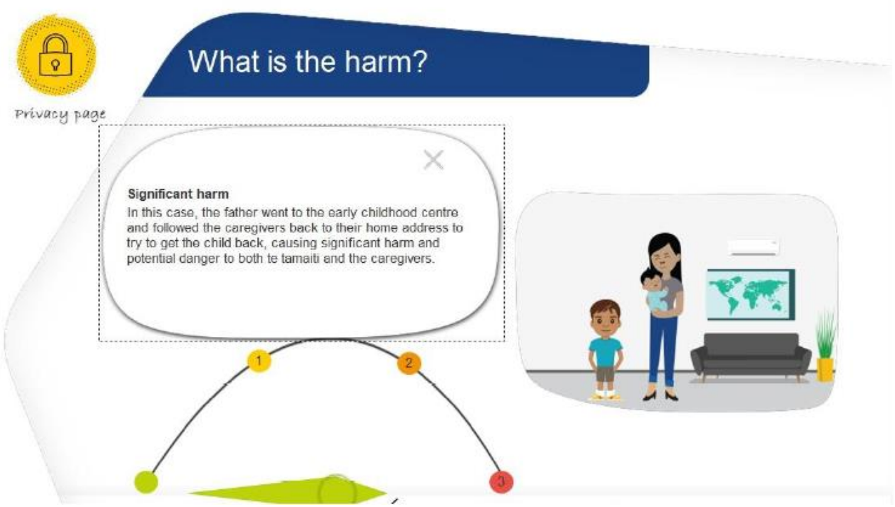


What is the harm?

Mia, a social worker, is updating a father about his child who is in care. In providing the update, she inadvertently mentions the name of the early childhood centre the child attends which is subject to a protection order (for the child and caregivers' safely).

What's the potential harm?

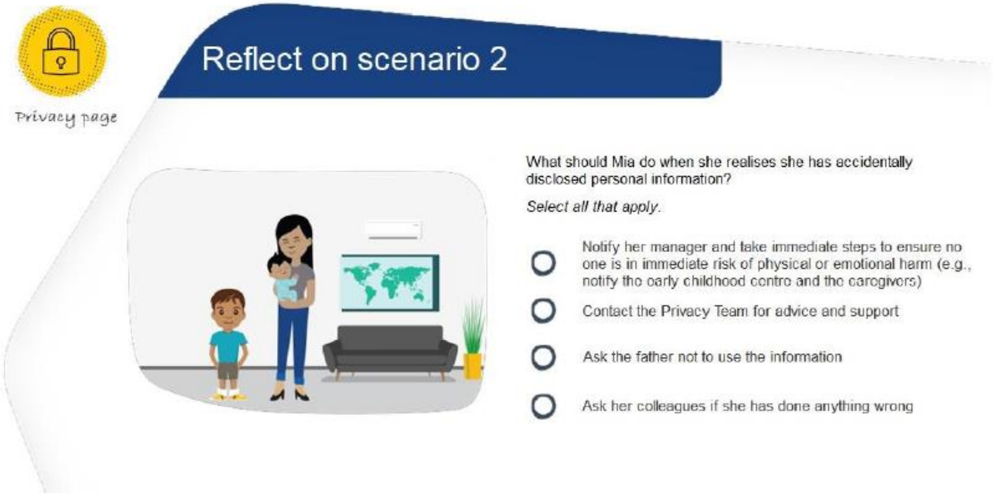
	 What is the harm? **Minimal harm** In this case, the father doesn't do anything with the information, so minimal harm is caused, for now  What is the harm? **Moderate harm** In this case, the father went to the early childhood centre and demanded to see te tamaiti, causing distress to all involved. 	



What is the harm?

Significant harm

In this case, the father went to the early childhood centre and followed the caregivers back to their home address to try to get the child back, causing significant harm and potential danger to both te tamaiti and the caregivers.



Reflect on scenario 2

What should Mia do when she realises she has accidentally disclosed personal information?

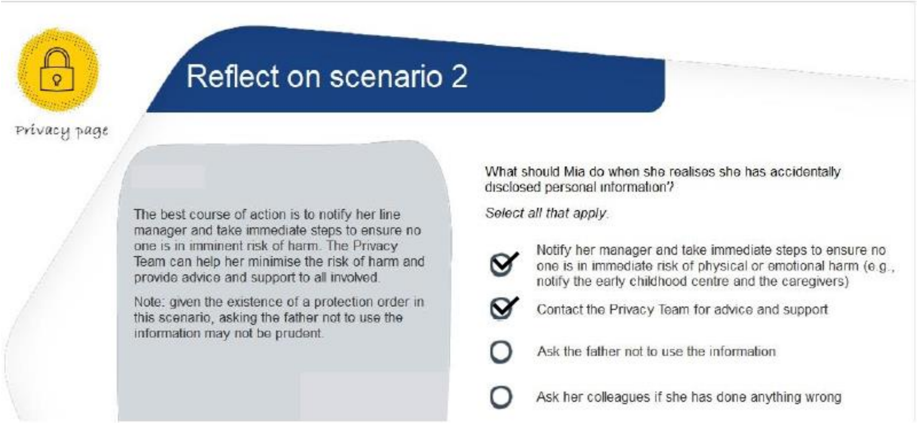
Select all that apply.

○ Notify her manager and take immediate steps to ensure no one is in immediate risk of physical or emotional harm (e.g., notify the early childhood centre and the caregivers)

○ Contact the Privacy Team for advice and support

○ Ask the father not to use the information

○ Ask her colleagues if she has done anything wrong



Reflect on scenario 2

The best course of action is to notify her line manager and take immediate steps to ensure no one is in imminent risk of harm. The Privacy Team can help her minimise the risk of harm and provide advice and support to all involved.

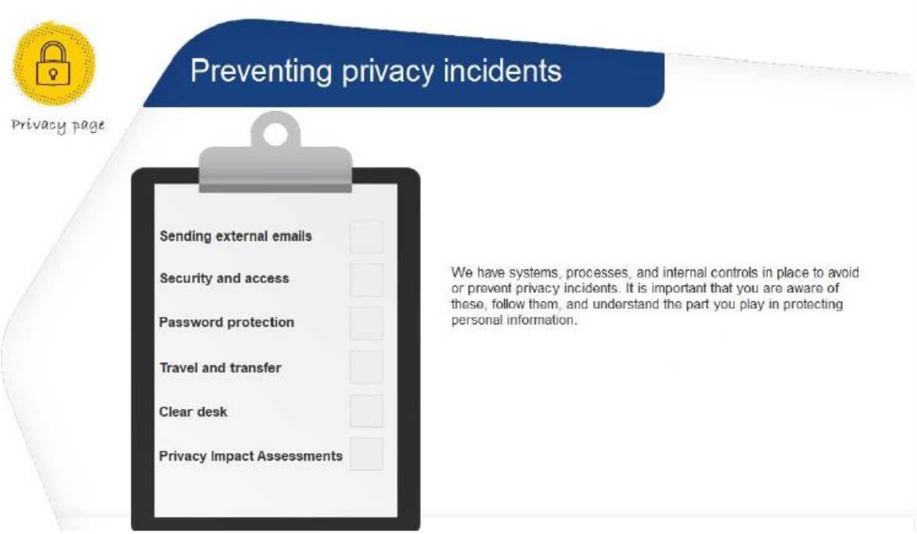
Note: given the existence of a protection order in this scenario, asking the father not to use the information may not be prudent.

What should Mia do when she realises she has accidentally disclosed personal information?

Select all that apply.

- ☑ Notify her manager and take immediate steps to ensure no one is in immediate risk of physical or emotional harm (e.g., notify the early childhood centre and the caregivers)
- ☑ Contact the Privacy Team for advice and support
- ○ Ask the father not to use the information
- ○ Ask her colleagues if she has done anything wrong

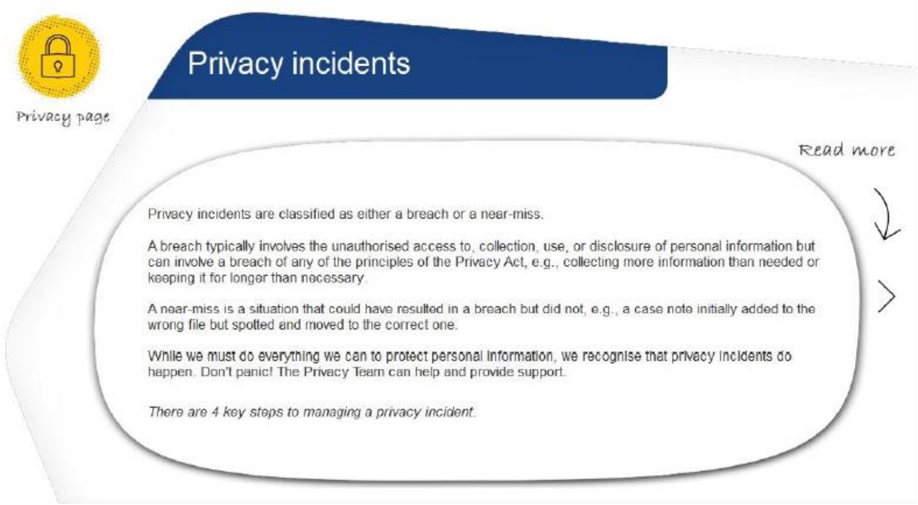
4. How to prevent and/or manage privacy incidents, for example:



Preventing privacy incidents

- Sending external emails □
- Security and access □
- Password protection □
- Travel and transfer □
- Clear desk □
- Privacy Impact Assessments □

We have systems, processes, and internal controls in place to avoid or prevent privacy incidents. It is important that you are aware of these, follow them, and understand the part you play in protecting personal information.

<table>
<tr>
<td></td>
<td>


Privacy incidents

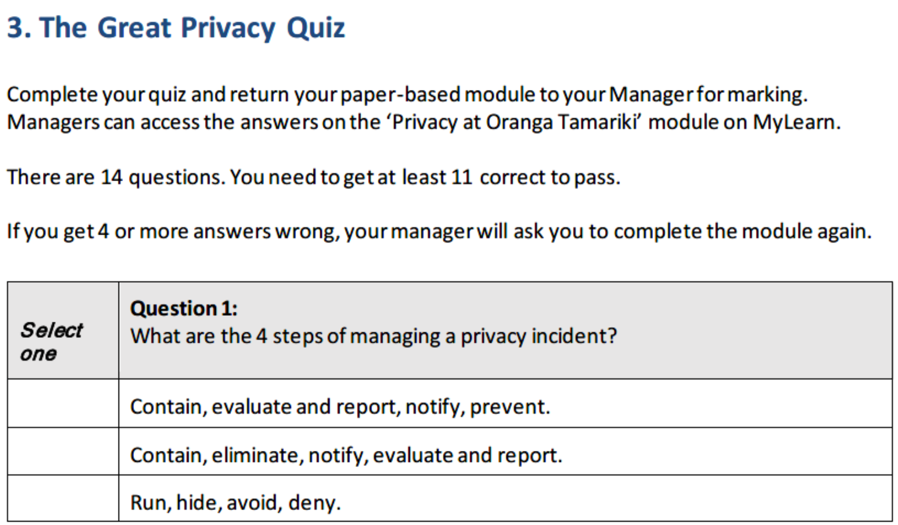
Privacy incidents are classified as either a breach or a near-miss.

A breach typically involves the unauthorised access to, collection, use, or disclosure of personal information but can involve a breach of any of the principles of the Privacy Act, e.g., collecting more information than needed or keeping it for longer than necessary.

A near-miss is a situation that could have resulted in a breach but did not, e.g., a case note initially added to the wrong file but spotted and moved to the correct one.

While we must do everything we can to protect personal information, we recognise that privacy incidents do happen. Don't panic! The Privacy Team can help and provide support.

There are 4 key steps to managing a privacy incident.



<b>3. The Great Privacy Quiz</b>

Complete your quiz and return your paper-based module to your Manager for marking.
Managers can access the answers on the ‘Privacy at Oranga Tamariki’ module on MyLearn.

There are 14 questions. You need to get at least 11 correct to pass.

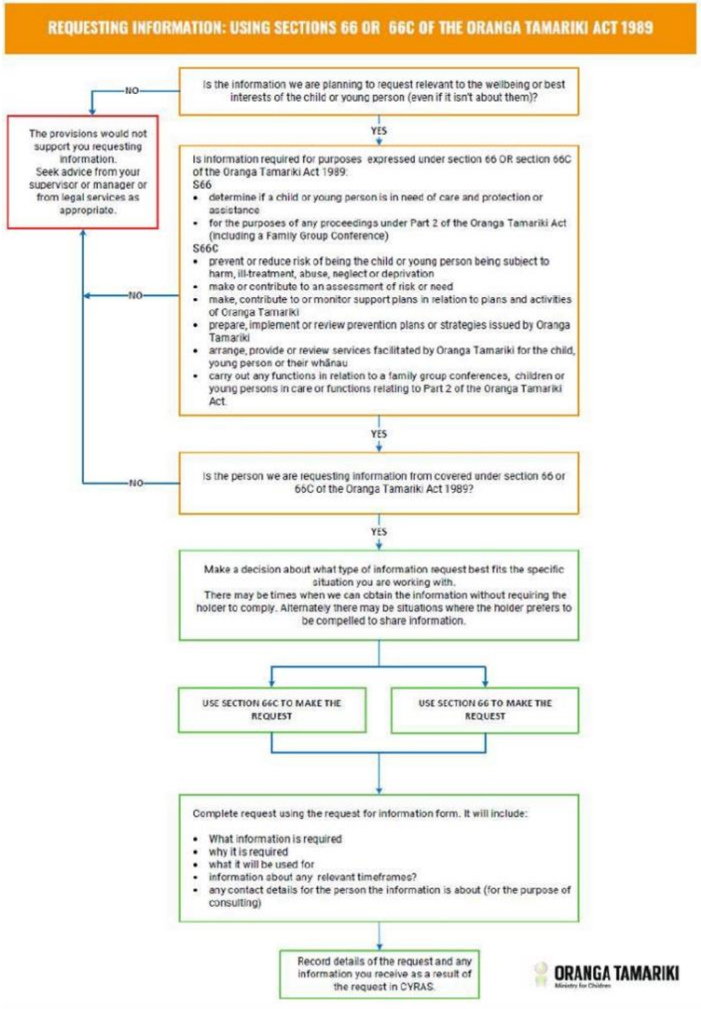
If you get 4 or more answers wrong, your manager will ask you to complete the module again.

<table>
<tr><th><i>Select one</i></th><th>Question 1:
What are the 4 steps of managing a privacy incident?</th></tr>
<tr><td></td><td>Contain, evaluate and report, notify, prevent.</td></tr>
<tr><td></td><td>Contain, eliminate, notify, evaluate and report.</td></tr>
<tr><td></td><td>Run, hide, avoid, deny.</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td><b>Information Sharing</b></td>
<td>This course deals with how to use the information provisions, ss 65A and 66, of the Oranga Tamariki Act. These provisions allow kaimahi to confidently request and disclose to support the wellbeing and best interests of tamariki and whānau. The document sets out:

- Why share information?
- Who can use the provisions?
</td>
<td>Contains reference to the old Privacy Act (1993)</td>
</tr>
</table>

- Purposes of sharing information
- When to use the information sharing provisions
- What do s 66 and 66c allow?
- How do you choose when to use each section?

Requesting information:



REQUESTING INFORMATION: USING SECTIONS 66 OR 66C OF THE ORANGA TAMARIKI ACT 1989

Is the information we are planning to request relevant to the wellbeing or best interests of the child or young person (even if it isn't about them)?

The provisions would not support you requesting information.
Seek advice from your supervisor or manager or from legal services as appropriate.

Is information required for purposes expressed under section 66 OR section 66C of the Oranga Tamariki Act 1989:

S66

- determine if a child or young person is in need of care and protection or assistance
- for the purposes of any proceedings under Part 2 of the Oranga Tamariki Act (including a Family Group Conference)

S66C

- prevent or reduce risk of being the child or young person being subject to harm, ill-treatment, abuse, neglect or deprivation
- make or contribute to an assessment of risk or need
- make, contribute to or monitor support plans in relation to plans and activities of Oranga Tamariki
- prepare, implement or review prevention plans or strategies issued by Oranga Tamariki
- arrange, provide or review services facilitated by Oranga Tamariki for the child, young person or their whānau
- carry out any functions in relation to a family group conferences, children or young persons in care or functions relating to Part 2 of the Oranga Tamariki Act.

Is the person we are requesting information from covered under section 66 or 66C of the Oranga Tamariki Act 1989?

Make a decision about what type of information request best fits the specific situation you are working with.
There may be times when we can obtain the information without requiring the holder to comply. Alternately there may be situations where the holder prefers to be compelled to share information.

USE SECTION 66C TO MAKE THE REQUEST

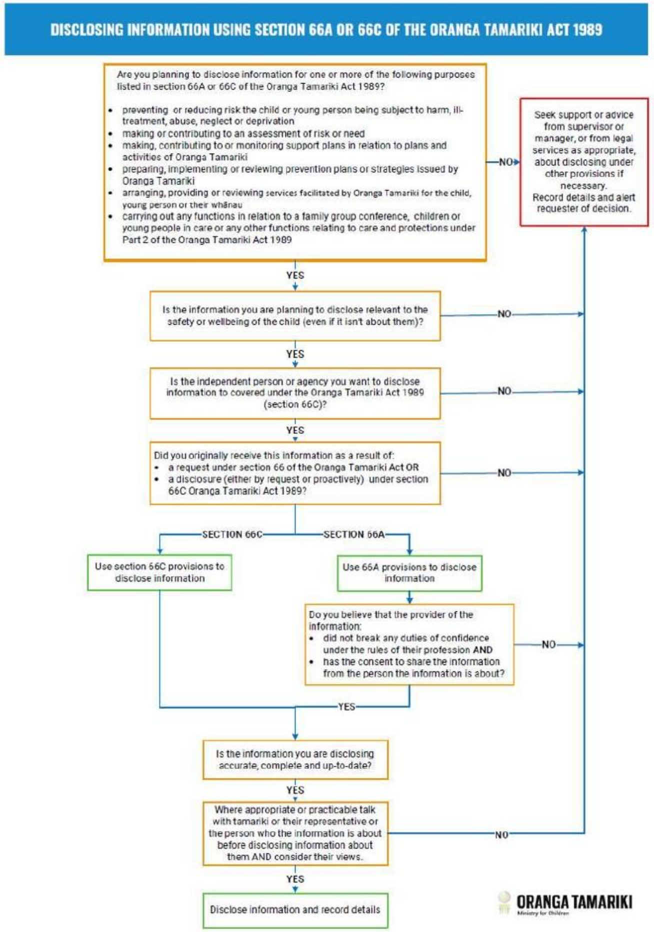
USE SECTION 66 TO MAKE THE REQUEST

Complete request using the request for information form. It will include:

- What information is required
- why it is required
- what it will be used for
- information about any relevant timeframes?
- any contact details for the person the information is about (for the purpose of consulting)

Record details of the request and any information you receive as a result of the request in CYRAS.

Receiving requests for information:



DISCLOSING INFORMATION USING SECTION 66A OR 66C OF THE ORANGA TAMARIKI ACT 1989

Are you planning to disclose information for one or more of the following purposes listed in section 66A or 66C of the Oranga Tamariki Act 1989?

- preventing or reducing risk the child or young person being subject to harm, ill-treatment, abuse, neglect or deprivation
- making or contributing to an assessment of risk or need
- making, contributing to or monitoring support plans in relation to plans and activities of Oranga Tamariki
- preparing, implementing or reviewing prevention plans or strategies issued by Oranga Tamariki
- arranging, providing or reviewing services facilitated by Oranga Tamariki for the child, young person or their whānau
- carrying out any functions in relation to a family group conference, children or young people in care or any other functions relating to care and protections under Part 2 of the Oranga Tamariki Act 1989

Seek support or advice from supervisor or manager, or from legal services as appropriate, about disclosing under other provisions if necessary.
Record details and alert requester of decision.

Is the information you are planning to disclose relevant to the safety or wellbeing of the child (even if it isn't about them)?

Is the independent person or agency you want to disclose information to covered under the Oranga Tamariki Act 1989 (section 66C)?

Did you originally receive this information as a result of:

- a request under section 66 of the Oranga Tamariki Act OR
- a disclosure (either by request or proactively) under section 66C Oranga Tamariki Act 1989?

Use section 66C provisions to disclose information

Use 66A provisions to disclose information

Do you believe that the provider of the information:

- did not break any duties of confidence under the rules of their profession AND
- has the consent to share the information from the person the information is about?

Is the information you are disclosing accurate, complete and up-to-date?

Where appropriate or practicable talk with tamariki or their representative or the person who the information is about before disclosing information about them AND consider their views.

Disclose information and record details

ORANGA TAMARIKI
Ministry for Children

Disclosing information safely: Disclosing information to others needs to be done in a way that makes the transfer of information as secure as possible.

	Keeping records: It is important to have records available for tamariki and whānau (or anyone else whose information is shared) to access so they can understand what has happened with their information. Records also provide a paper trail for us if anyone wants to understand the decisions we make around sharing information (which is important if we are questioned about sharing or there is a complaint). Case notes: Case notes should include details of the information requested, received, or disclosed; who the information came from or was shared with and the reasons for this. Case notes on your consultation with te tamaiti or the persons concerned should detail how the consultation occurred, their views on the information proposed to be disclosed, how these views were taken into account. If a decision has been made to disclose the information against their wishes the rationale for this must be included. Guidance on consulting with tamariki is included.	