5 December 2019

# Final Report

# Independent Review of the Tuia 250 Voyage Trainee Privacy Breach

# Manatū Taonga – Ministry for Culture and Heritage

RDC Group Ltd

# Contents

# Introduction

## This report provides Manatū Taonga, the Ministry for Culture and Heritage with an independent review of the decisions and processes relating to the procurement and management of the Tuia 250 website and the circumstances that led to the breach of the privacy of applicants for the trainee crew programme.

### 1. The issues in scope of this review

On 30 August 2019, the Chief Executive of Manatū Taonga, the Ministry for Culture and Heritage (MCH) commissioned an independent review of MCH's systems, processes and the circumstances that led to a breach of the personal information of most of the applicants for the Tuia 250 trainee crew programme. This review also includes an independent assessment of the procurement and management of the Tuia 250 website which was used to receive those applications.

In particular, the review covered:

1. Governance and management of the Tuia 250 trainee crew programme relating to:
   (a) The decision to use an externally built and hosted website to receive applications for trainee crew members
   (b) The management of personal information
   (c) The identification and management of risks regarding management of personal information.
2. The procurement process including:
   (a) Analysis of technical requirements
   (b) Analysis of potential supplier proposals
   (c) Selection of preferred supplier
   (d) Contractual arrangements between MCH and the Supplier including the brief, agreed technical specifications, and variations to create the online application function
   (e) Management of the contract and relationship with the Supplier throughout the duration of the work.
3. The Tuia 250 website itself, in particular technical functionality with respect to information security and management of personal information.
4. The timeline of the breach, including when and how it was identified by the MCH.
5. Whether MCH adhered to its internal policies and to applicable government policies and good practice guidance.

## 2. Objectives of this review and our approach

The objectives of this review were to:

a. Build a comprehensive understanding of the situation and cause of the privacy breach; and

b. Fully investigate these, to make findings about the facts, provide an analysis to determine what caused the breach, to identify lessons learned and to make recommendations on changes and improvements needed to avoid a similar breach in future.

In undertaking this review, we:

a. Looked at the documentation surrounding the procurement of the Supplier of the Tuia 250 website.

b. Interviewed relevant staff, management and external parties (Appendix 1).

c. Reviewed Ministry internal policies and other applicable government policies and good practice guidelines.

d. Were unable to review logs of activity on the Tuia 250 Encounters website from the commencement of the breach because these were not kept beyond a 5-day period.

e. Were unable to view a working copy of the Tuia 250 Encounters website because it had, quite properly, been taken down.

## 3. Limitations of this review and acknowledgements

In line with our Terms of Reference (Appendix 2), we do not make any findings nor make any comment on:

- The governance and management of the wider Tuia 250 programme to the extent that this can be separated from the governance and management of the trainee crew programme.
- The Ministry's main website or other digital assets.
- The response to the privacy breach itself, once the Ministry became aware of it.
- Third party actions arising from the breach, such as unauthorised use of personal information.
- The conduct or professional performance of any individual manager or staff members.

We would like to acknowledge the thoughtful, open and constructive input from all those who contributed to this review. We gained a clear sense of the genuine desire of everyone involved to understand what the lessons are to be taken out of the events that led to the privacy breach and to better understand what can be done to ensure a similar occurrence cannot happen again.

## 4. Context and background of Tuia 250

Cabinet first approved the Tuia - Encounters 250 (Tuia 250) commemoration as a Tier 1 (major) anniversary in 2015. Recognition of, and respect for, the different perspectives on this historical event, including perspectives on the damage this event caused to the indigenous population and the way that this event has historically been portrayed within Aotearoa New Zealand, meant that this commemoration was always going to be challenging.

Tuia 250 is a commemoration of Aotearoa New Zealand's pacific voyaging heritage and acknowledges the first onshore encounters between Māori and Pākehā in 1769-70.

One of the most important aspects of Tuia 250 is a flotilla of waka hourua, va'a tipaerua and tall ships sailing the coast from October 2019 to December 2019, landing at 15 communities. This is known as the Tuia 250 Voyage. MCH determined that the best way to promote the Tuia 250 Voyage was through a website and to provide interactive materials for people to experience the voyaging aspect of Tuia 250 Encounters. The functionality of the website allows people to track the voyage of the flotilla to and around Aotearoa New Zealand.

MCH is relatively sophisticated when it comes to designing and creating websites as well as generating content for them. At the time this report was prepared, MCH has 10 websites connected with its core business. This includes the main corporate information site for MCH, and an additional 9 websites connected with research and publishing and various commemorations that MCH has responsibility for or is associated with. It should be noted that one of these sites is a blog connected with the same subject matter as another website. However, as it has a different Content Management System (CMS) it is counted as a separate website for the purposes of this report.

As a generalisation, the purpose of the Ministry's sites is to promote and provide information about the subject matter to which they relate. They are generally not used for the collection, storage and use of personal information by MCH.

MCH is relatively inexperienced when it comes to the storage and use of personal information. It does not form part of MCH's usual course of business in the web environment. Unlike some other government agencies, MCH does *not* have large operational units interacting with the public and it does *not* routinely collect, use or store personal information from people outside of the Ministry. MCH assessed itself as "a small, low risk agency" in the GCPO Privacy Self-Assessment 2018-2019.

# Analysis

## 5. Governance and management of the Tuia 250 Voyage trainee crew programme

The structure for the delivery of Tuia 250 was determined by Cabinet.

A National Coordinating Committee (NCC) for Tuia 250 was established at the outset. The NCC is co-chaired by Hoturoa Barclay-Kerr and Dame Jenny Shipley. The purpose of the NCC is to ensure a cohesive and coordinated national programme of activities. The NCC provides advice to agencies and to Ministers.

A governance structure was established that included MCH chairing a Governmental Working Group. That working group consisted of the following government agencies:

- *Manatū Taonga, Ministry for Culture and Heritage (Chair)*
- *Te Papa Atawhai, Department of Conservation,*
- *Te Puni Kokiri, Ministry of Māori Development,*
- *Te Tari Taiwhenua, Department of Internal Affairs,*
- *Manatū Aorere, Ministry of Foreign Affairs and Trade,*
- *Hīkina Whakatutuki, Ministry of Business Innovation and Employment (MBIE),*
- *Te Ope Kātua o Aotearoa, the New Zealand Defence Force,*
- *Pouhere Taonga, Heritage New Zealand,*
- *Te Tari o te Pirimia me te Rūnanga Kāwanatanga, Department of the Prime Minister and Cabinet,*

- *Te Manatū mō Ngā Iwi o Te Moana-nui-a-Kiwa, Ministry for Pacific Peoples,*
- *Toitū Te Whenua, Land Information New Zealand,*
- *Museum of New Zealand Te Papa Tongarewa, and*
- *Te Tāhuhu o te Mātauranga, Ministry of Education.*

The purpose of this working group was to ensure an All-of-Government approach was taken to the planning and delivery of the Tuia 250 commemorations.

In addition, a Risk Steering Group (RSG) was created. The role of the RSG was to provide specialist advice and support to the Tuia 250 Sponsor and Project Director on the 'whole of Tuia 250' risks (including operational arrangements and contingency planning of regional events). The RSG was responsible for advice and support to managing all Tuia 250 project risk that falls under the responsibility of MCH or could cause significant reputational damage to MCH.

The membership of the RSG is as follows:

- *MCH was also the Chair of the RSG*
- *Police as the lead agency for security and public safety*
- *The Department of Prime Minister and Cabinet (DPMC) to provide the key conduit to the national system and ODESC (Officials Committee for Domestic and External Security Coordination)*
- *MBIE (Major Events)*
- *Nō te rere moana Aotearoa, Maritime New Zealand*
- *Other agencies as required.*

MCH's role in Tuia 250 is to plan, establish and support a flotilla and voyage around Aotearoa New Zealand. The total budget for Tuia 250 is $13.93 million.

The critical success factors for Tuia 250 are:

- *There is a positive national engagement with Tuia 250.*
- *The Tuia 250 national voyaging event is delivered safely and successfully.*
- *Tuia 250 brings to life the exceptional voyaging feats of Pacific, Māori and European voyaging communities.*
- *Māori communities become more confident that the historical context and mamae (pain) associated with commemoration has been managed appropriately.*
- *All New Zealand children have an increased understanding of Aotearoa New Zealand's history, our place in the Pacific and see themselves and their heritage reflected positively and valued in our national diversity.*

The Tuia 250 Voyage Trainee Crew Programme (Tuia Trainee Programme) was a component of the Tuia 250 programme. The Tuia 250 programme is out of the scope of this review to the extent that it can be separated from the Tuia Trainee Programme. The Tuia Trainee Programme allowed people to apply online for 450 berths that were available on the Tuia 250 flotilla voyages.

The Tuia Trainee Programme was not managed as a separate project from Tuia 250. It was managed as a part of the Tuia 250 project. Despite the cross-government governance arrangements in place, the Tuia Trainee Programme did not seem to have any visibility beyond MCH in terms of decision-making for the application process, although advice was sought and given to other aspects of the Tuia Trainee Programme including the safety risks of trainees.

The Tuia 250 documentation that we have seen suggests that the information of trainees and associated plans for managing this part of the programme was the responsibility of the *Crew/Trainee Berth Coordinator*. Information related to trainees was to be protected by being classified as "restricted access" according to these plans.

Otherwise the general focus with respect to personal information was on managing physical risks to trainees once their applications had been approved rather than on any risk to their personal information as a result of its management by MCH or its suppliers.

Risks to privacy and personal information was not identified as a stand-alone risk on any risk register that we have seen relating to Tuia 250.

## 6. Procurement process for the Tuia 250 website

***Background***

The procurement process for the Tuia 250 website commenced in July 2018. The first procurement plan proposed a direct source procurement process, with MCH seeking a proposal from one supplier. We were advised that this process was initially proposed due to the specific nature and requirements of the Tuia 250 website. In particular, the requirements relating to the Tuia 250 Voyage and flotilla tracking specialist section of the proposed website.

***Procurement Plan***

A potential supplier was identified to MCH by an MCH staff member familiar with the supplier's work. The staff member suggested that the supplier would be able to provide the type of website MCH needed, in particular for the voyaging aspect of the Tuia 250 website. There was a pre-existing connection and professional relationship between the proposed supplier and the MCH staff member. This connection between the staff member and the supplier was known to some staff and management within the Tuia 250 programme, although we have not seen any evidence this was ever formally declared or recorded as part of the website procurement process. We are unaware if Tuia 250 management or procurement staff provided any guidance or training on how to manage this association through a procurement process. We also note this staff member was relatively new to the public service.

A draft procurement plan proposing direct sourcing from this supplier was then prepared.

Legal and Finance staff in MCH were consulted as required in the procurement process. Their advice was that direct source procurement was not appropriate and should be discontinued. Specialist procurement assistance and advice was then obtained and provided for the rest of the procurement process. The MCH staff member who knew the supplier did not play any further part in the decision-making processes that related to the procurement of the supplier, although they did provide information to the supplier relating to the requirements of the voyaging component of the website.

Among initial advice sought was whether MCH, as a smaller Ministry, would need to comply with the All-of-Government Procurement Process. This may have required MCH to seek proposals only from approved suppliers on the common capability panel which MCH was a party to under the common capability contract. MCH sought advice from DIA procurement staff. MCH advised DIA of the particular needs of the Tuia 250 website and on the procurement process they were thinking of following. The outcome was advice that MCH could source suppliers for the Tuia 250 website from a range of suppliers and was not limited to suppliers on the panel.

Following receipt of this advice, a further procurement plan was developed which was approved on 18 September 2018. The procurement plan identified the following relevant requirements:

- *The website was to be contracted to 2 suppliers due to the scope and unique design aspects of the site.*
- *The first supplier was responsible for the main design, implementation, hosting and maintenance services for the site.*
- *The estimated value for the services of the first supplier was budgeted at $90,000.00 plus GST.*
- *A second supplier under a separate contract was to provide voyage tracking, live streaming, and app design technology tools to feed into overall website design. The suppliers would be required to work together at times, but each was to have separate areas of responsibility and deliverables. A separate procurement plan for this aspect of the site was to be developed.*
- *Proposals would be sought from three suppliers identified as having the relevant experience and expertise required.*
- *Evaluation of the proposals received was to be assessed against the following criteria:*
    - *Proposed approach and methodology*
    - *Proven capability to deliver including the skills and experience of personnel*
    - *Ability to meet timeframes*
    - *Value for money.*
- *A three-person panel was proposed to evaluate supplier proposals with additional technical assistance to be provided from MCH's IT and Legal staff as required.*
- *Some general specifications for the website were included. However, none of these related to the Voyage Trainee Application process. They were:*
    - *Information*
    - *Education page*
    - *Event calendar*
    - *Media resource and accreditation section*
    - *Whata Kōrero – a platform for stories connected with the commemoration*
    - *Voyaging event information and connections.*
- *The website would be delivered in two phases. Phase One related to information on the objectives and components of the commemoration and events (completed by 15 November 2018), a media section and platform for stories, and links to websites of government department partners and landing site trusts. Phase Two was to include staged release of voyaging event components.*
- *Any contract with the Supplier was to be on the standard terms and conditions of MCH unless the terms and conditions of any successful supplier offered a better fit for the engagement.*
- *Probity conditions were also included in the procurement plan.*
- *There was no reference to the standard requirements for websites in terms of accessibility or other common requirements for government websites in the contract.*

***RFP Process***

Following approval of the procurement plan, a Request for Proposals (RFP) process was initiated by MCH. An RFP was drafted, approved and sent to three prospective suppliers on 1 October 2018 with a closing date of 15 October 2018. The RFP relevantly sought proposals essentially in line with the approved procurement plan for Phases One and Two of the Tuia

250 website. Hosting of the site was at the discretion of MCH, meaning that MCH could opt to use existing facilities available to it to host the site, or it could agree that the successful supplier could host it.

There is no reference to the Voyage Trainee Application Process that subsequently led to the data breach. This did not form part of the procurement process. In addition, information was sought from suppliers about their experience in "GPS based tracking and live streaming". This area is described as "out of scope of the RFP". We were told that this related to the Tuia 250 Voyage component of the website and Tuia 250 commemorations more broadly.

One of the three suppliers that MCH approached to respond to its RFP was a supplier on the DIA All-of-Government contract. Two of the suppliers were suppliers that MCH had previously worked with. Proposals were received within timeframes from all three of the suppliers.

We believe that the MCH staff member who had a pre-existing relationship with one of the suppliers assisted that supplier to prepare their response to the RFP. This is based on what we concluded from our separate interviews with the staff member and the Supplier. It was clear to us that the staff member had a previous working and connected relationship with the Supplier which meant the staff member was well aware of the capabilities of that Supplier. As already noted, we are not aware if the staff member was provided with guidance or counselling as to how their interest in having a pre-existing professional relationship should be managed. The staff member was clearly of the view that the Supplier had skill and experience with voyaging, that would be of benefit to the Tuia 250 programme and the development of the website in particular. We believe that the staff member was providing assistance to the Supplier with the best of intentions and was not aware that this might create a perception of unfair assistance or was otherwise inappropriate. While some of what we were told was inconsistent, on balance we concluded the MCH staff member provided assistance to the successful Supplier in the course of the Supplier submitting their proposal. We note too that this Supplier was successful in securing the contract to build the Tuia 250 website.

While assisting suppliers to respond to RFPs does not in itself represent a conflict of interest, it is not good practice to only provide assistance to one supplier. We understand that this assistance was provided because the Supplier was inexperienced in responding to government tenders and the assistance was to ensure they could operate on a more level playing field. Again, this assistance does not appear to have been formally declared nor made known to Tuia 250 management.

***Evaluation of proposals***

A five-person procurement panel was convened, and a standard procurement process followed. The panel met and the selection process commenced. The panel sought additional information from all three suppliers through the Chair of the panel. The information sought was provided within required timeframes. The panel considered these additional materials, completed deliberations and a preferred supplier was identified using the scoring system devised to assess proposals. We consider that this was an appropriate selection process and is in line with procurement processes set out in the project plan for Tuia 250.

A written recommendation dated 25 October 2018 was produced and forwarded to the Deputy Chief Executive-Tuia 250. The reasons for selecting the Supplier are summarised by us as the Supplier:

- *Scored the highest using the scoring system of the panel. However, there was not a big difference between the scores of all suppliers (1.125 points separated the successful Supplier from the next bid out of a maximum of 50 points).*
- *Submitted a proposal that was under budget. The two other suppliers were over budget.*
- *Has previous experience working on platforms for waka voyages and voyaging projects*

*– a base design and tools were available and would not be required to be developed. This would appear to be outside the scope of the RFP however it is clearly related to the requirements for the Tuia 250 commemorations.*

- *Included providing training for MCH staff in Wellington in the costs of the proposal.*

***Contract to Build the Website***

Following approval of the recommendation by the Deputy Chief Executive -Tuia 250, a contract was drafted and executed by the Supplier and the Deputy Chief Executive -Tuia 250. The contract was to supply the Tuia 250 website to MCH. That contract was signed by the parties on 5 December 2018. It should be noted that the contract was therefore signed after the key dates for delivery of some of the Tuia 250 website project had passed. In particular, the November 2018 deadline had passed. The contract was signed using standard forms, incorporates government standard conditions for the provision of services and had the following relevant terms:

- *It has a start date of 26 November 2018 and an end date of June 2020.*
- *There were two phases of the website development, broadly in line with previous requirements and these were split into 10 deliverables. Phase One related to information on the objectives and components of the commemoration and events. Phase Two was to include staged release of voyaging event components.*
- *Phase Two included some of the Tuia 250 Voyage component of the website which was originally envisioned in previous documentation as a separate procurement process and was to be provided by a separate supplier.*
- *There was no increase to payment due under the contract.*
- *Payments were to be made to the Supplier in line with the completion of deliverables. Timeframes were specified for the completion of the deliverables.*
- *Government standard terms and conditions in the contract included the provision that "If the nature of the services requires it, the Supplier will deliver services…that respects the personal privacy and dignity of all participants and stakeholders".*

This is the last formal document that describes the relationship between MCH and the Supplier. Any other variation or agreement to amend the relationship was verbal or took place in emails and was agreed between the Supplier and MCH.

This includes the implementation of the decision to use the Tuia 250 website to receive Tuia Voyage Trainee applications. There is no formal variation to the contract between MCH and the Supplier that related to the decision to create the online application function that relates to the breach. This is a significant variation, both to the nature of the website which, up until this point was a website designed to distribute as much information as possible by way of promotion. The addition of an application function to collect information, including quite sensitive personal information in many cases, was a significant and important change in the requirements and should have been managed in a more considered manner.

It is also important to note that the Supplier provided hosting of the Tuia 250 website through a third-party web hosting provider. It was not hosted on MCH servers even though the contract allowed for that. It appears to have been agreed by the parties after the execution of the contract that the Supplier would host the website.

***Management of the contractual relationship with the Supplier***

There was no single point of contact at MCH for the Supplier, although contact generally was more frequent with staff and management from the Tuia 250 team, including the Deputy Chief Executive - Tuia 250 as well as the web team[1]. There was a single supplier point of

[1] The Web Team became the Production Team in November 2014, part of the Research and Publishing Group in the Delivery Group.

contact for MCH staff.

There were interactions with the Supplier from a number of different MCH staff. These staff were mainly based in the Tuia 250 team and later the Production (Web Design) Team.

We were told that instructions MCH gave were complied with for the most part, that content was posted to the site and as concerns with the look and feel of the site were raised between MCH and the Supplier, access to the CMS to directly post and design pages that held content was provided by the Supplier to MCH staff. MCH staff were not overly familiar with the CMS employed by the Supplier, and assistance to deal with issues that arose with the appearance of content and page design in that CMS was required. The Supplier provided that assistance to ensure that the website would function, and content was placed on the site with the minimum of delay. The Supplier also provided MCH staff with training in Wellington as required under the contract.

***The decision to use an externally built and hosted website to receive applications for trainee crew member positions***

The decision to use an externally built and hosted website to receive applications for trainee crew members was not part of the original procurement process for the Tuia 250 website. It was not part of the RFP and therefore not included in the proposals that were received by MCH. It follows that it was not a requirement of the contract with the successful supplier.

Using the website for this purpose was not therefore considered as part of the wider Tuia 250 project planning, governance and risk management processes. By virtue of the various communications and agreements made between the Supplier and MCH it was subsequently incorporated into the contractual relationship between the parties, notwithstanding that this was never formally reflected in a variation to the contract.

The Ministry's *Creating and Managing Ministry Websites – Guidelines*, do not contain any specific references to creating websites that collect personal information, but does require that any new website must be referred to and discussed with both the Communications Team, the CIO's team, and the Web Manager in MCH. These guidelines are dated 2011 and were out of date as they refer to the Web Development Team reporting to the CIO, whereas the Production Team (formerly the Web Team) is part of the Research and Publishing Group in the Delivery Group. The Privacy Officer sits within the CIO's team.

While the guidelines were out of date, the 2017 Digital Strategy provided detailed guidance on establishing websites and the Ministry's related policies, all of which should have been considered when establishing and managing the Tuia 250 website. The Digital Strategy refers to the privacy principles, contains a link to information on those principles, and identifies the Privacy Officer as a point of contact. There are also links to the relevant Information and Records Management policy in the CIO's team.

Because the initial website procurement scope did not include the online application process, the approval within MCH would not have considered this functionality and any risks associated with it. We are not aware that the use of the website for managing applications was ever formally raised with senior management outside of the Tuia 250 programme. The Deputy Chief Executive – Tuia 250 made the decision to use the website for the voyage applications. It seems clear, however, that senior management outside of Tuia 250 were not aware of this use of the website until after the breach had occurred.

There is no suggestion that there was any issue raised within MCH or by the Supplier to the use of the website to host a webform to help manage the applications for crew positions. Nor did we find any indication that this could not be successfully executed by the Supplier. The Supplier undertook steps to ensure that the webform could be deployed via the website and did not express any concerns about the security of the information being collected via the webform at the time. Later, in response to concerns raised by MCH, the Supplier conveyed assurances relating to the security settings and systems in place to safeguard the website. We consider the Supplier was genuine and responsive to the concerns raised and

like MCH, was unaware there was a problem with the security settings on individual files.

From the documentation that we have been able to review, and from our interviews, it seems that the decision to use the website to host an application form was made in early May 2019. The decision was not made as part of any formal governance process, but rather as one of many day-to-day decisions being made within the Tuia 250 programme. Senior managers outside of the Tuia 250 programme were not involved which we were told is not unusual practice for MCH's operating model. It was unclear to us from the documentation we reviewed who the individual was within the Tuia 250 program that actually made the decision to use the form. This was clarified in the interviews that we conducted and highlights an issue of appropriate record keeping and documentation within the programme.

Much of the implementation relating to the form was undertaken by the Supplier and junior staff at MCH. While some senior management at MCH were aware of this decision, the demands of the wider Tuia 250 project, the limited resources available to MCH, and the focus on managing parties crucial to the success of Tuia 250, meant that the implementation of the decision to use the webform on the external website was left to relatively junior staff and the Supplier, with input from other Ministry staff as needed. Management oversight, particularly within the Tui 250 program appeared to us to be weak given the risks involved.

***Implementation of the application form on the website***

The implementation of the online application required a webform to be deployed on the website. Applicants for trainee crew positions would use the form to provide their application details and to upload documentation to support their application (for the most part these were documents to confirm identity). This information would allow MCH to make assessments of eligibility based on the information received both from the form and any uploaded documents.

Implementation steps included the design of the webform, approval of it, and deploying it to the website with the required plugin or module that would allow the webform to function on the CMS utilised for the Tuia 250 website. Our understanding of the web form and plugin is that they worked together to allow applicants to enter the required information and upload documentation to support their application.

The webform was deployed on the Tuia 250 website on the 28th of May 2019. Documents uploaded by applicants using the Tuia Trainee online application process were stored in the media library, or folder, of the Tuia 250 website. Other personal information in the form was stored elsewhere.

It is important to note that there is nothing inherently wrong in employing a webform on the externally hosted site for the purposes of the trainee crew programme. Government agencies collect personal information from the public through websites routinely. This may not always be done through externally hosted websites, however the error giving rise to the privacy breach in this case does not appear to relate to the hosting of the site. The fault was caused by incorrect access settings on the folder on the website which stored data uploaded during the application process. The access settings made the information in the folder discoverable for search engine indexing, and therefore available to anyone or search bots following the links the search engines created.

***Other procurement matters***

There are a number of other matters relating to the procurement process that we need to highlight. The first of these is that the activity logs, which record what has happened on the Tuia 250 website were only held for 4 days plus the day of recording (a total of 5 days). This meant that security specialists investigating access to the personal information after the breach was discovered were not able to ascertain what specific actions had been taken on the site by people or machines, except for the 5 days before the breach was discovered. For this reason, technical experts examining the site after the breach was discovered could only say that it was highly probable that all the folders had been indexed and searched and

therefore it was probable that all of people's personal information had been compromised.

This is inconsistent with the Supplier's reference in their response to the RFP to being able to maintain 12 months of activity logs. The web host being used by the Supplier offered this level of service. However, it appears that either this service-level was not initiated, or at some point it was deactivated during the course of the contract.

While this would not have affected the breach itself because the information was not secure regardless of the logs, it would have assisted experts to determine the extent and duration of the breach and potentially where applicants' personal information had been sent.

The second item of interest from a procurement perspective is the nature of the relationship between MCH and the Supplier by this stage. The contract specified clearly defined roles for each party to the contract, however these had become less clear as the contract ran its course. By this time, MCH had various levels of access to the site through the CMS in order to post content to the site and undertake tasks associated with the site independently of the Supplier. Coupled with the differences from the procurement plan, through to the contract, and then as that contract ran its course, there was a very different arrangement in place between the parties by the time the breach is discovered and the Tuia 250 website was taken down. While MCH had access to the server and was able to manage content and the look and feel of the website directly, they did not at any stage have access to the control panel, and therefore the ability to change global security settings.

Thirdly, there was at least one significant extension to the work that the Supplier had agreed to undertake. This was the Tuia Trainee Application process where the breach occurs. There was no formal variation to the contract to record this change. This was well short of good practice.

## 7. The Tuia 250 website - Information Security, Management of Personal Information and the Privacy Breach

The Tuia 250 website was designed for one main purpose; to provide as much information as possible about Tuia 250 and related events. The website was designed and configured to be as open and accessible as possible with the information stored on it. This was an important factor too because it sets up the nature and style of website and its dominant purpose.

Websites of this nature are often referred to as *brochure websites.* Every setting on these types of websites is configured to make access to the information on the site as streamlined as possible. This includes configuring files and information to make it easy for search engine indexing robots, or bots, to catalogue the information so that individuals and machines seeking access to the information can easily do so.

The information held by the site, by default, was intended to be for publication and to be widely available. As such, the default setting of the site was configured to facilitate this access to information and indexing by bots and search engines.

The security settings on the site itself were configured to protect the site from being hacked and/or the information on the site being changed or manipulated.

In May 2019 with the introduction of the application form, the purpose of the website was fundamentally changed. As well as still being a brochure site it was now also a point through which personal information associated with applications for the Tuia Trainee Programme was being collected and stored.

As already mentioned, there was no contractual variation to accommodate this new purpose. That was because some of the required functionality originally contracted for was now no longer required leaving sufficient budget to complete the changes relating to the applications. Further, the Supplier identified that they could accommodate the request to host the application form without too much difficulty and they confirmed they had the capacity to carry out the necessary tasks.

In setting up the form on the website, it seems most likely that the access permissions on the folders containing the application information uploaded by applicants were not changed or configured to reflect that these folders and the files within them held personal information. This information should not have been accessible to anyone or anything (including search bots) outside of the Ministry.

The issues with the security settings and the insecure storage of personal information could have been discovered and rectified if penetration testing of the website had been carried out before the application process went live.

***Concerns with Tuia 250 website***

In June 2019 concerns were raised about the Tuia 250 website in MCH. Broadly these concerns related to three areas:

- The design, look and feel of the website: These concerns can best be summarised as design concerns that the site does not look as good as it should and that the site was not consistent with the design standards of other MCH sites.
- Failure to comply with government standards for websites: these relate to accessibility requirements for such things as software utilised by people living with visual impairment for example and other standard requirements for government websites such as disclaimers and notices required, including privacy notices.
- Security of the CMS: these concerns related to the security of the system by which content is placed on the site and managed. In a broad sense the issue was the potential for hacking or taking over control of the website.

These concerns were raised with management within MCH, including managers beyond the Tuia 250 team. The decision was made to suspend the Tuia Trainee Programme section of the website while these concerns were investigated with the Supplier and other sources of information about the security of the CMS were explored. The Tuia Trainee Programme section of the website was closed on 8 June 2019.

The concerns were investigated within MCH and advice about the security of the CMS, server, website generally and specific questions about the security of personal information was sought from the Supplier. Assurances were received from the Supplier and enquiries of MCH staff themselves resulted in information being provided to management that satisfied decision-makers that the website with the Tuia Trainee Programme online application process could be reactivated to continue to receive applications. The website was reactivated on 12 June 2019.

Internal email correspondence and MCH records show that information management planning was still being undertaken after the Tuia Trainee Programme online application process had already commenced. This meant that files attached to the webform applications being made were being assessed for information management purposes while personal information, and in this case the breach, was already occurring. This is not best practice. Information management processes should have been completed before any personal information was collected.

Following the reinstatement of the Tuia Trainee Programme online application process, this process continued in operation past the original closing date of 16 June 2019 to an extended closing date of 26 June 2019. The reason for the extension of time was to allow for more applications to be received to ensure that all trainee positions were filled. After closing on 26 June 2019 all files uploaded with applications remained stored in the media library along with some additional files uploaded to the site in respect of applications received by MCH through other means (by email and post). This personal information remained in an insecure environment from the first deployment of the online application process until the website was taken down on 22 August 2019.

***The management of personal information and the privacy breach***

On the 28th of May 2019 the webform went live on the website to implement the Tuia Trainee Programme online application process. This is important as we did not see any evidence suggesting that the settings for the folder were ever changed to allow this access to the documents. Therefore, this access setting seems to have been applied to the folder where the personal information was stored throughout the collection and storage of this personal information.[2] As such, the breach was ongoing the entire time that the application form was available to be used. The breach probably began at the point the webform was deployed[3]. This is because any personal information that was uploaded would not have been stored securely[4]. It seems most likely that the incorrect settings were not the result of someone changing them from appropriate to inappropriate settings, but rather the default settings for the website folders holding personal information being left in the same "open" configuration as every other folder on the website. In short, for the folders holding personal information, the settings needed to be manually changed to a "secure" setting and they were not.

Appropriate management of personal information uploaded as a file attached to an application was lacking from the moment the form was deployed. The permissions for accessing the media library were configured to enable search engines to see and index everything in the media library. As a result, all the uploaded documents and associated personal information would have been indexed and copies of all the images (e.g. passports and driver licences etc..) made. Following which, this information would appear in any properly configured search of the search engines that had indexed the Tuia 250 website media library. The images would also appear in the search results of those search engines that had not indexed the Tuia 250 website, if they used the indexing services of search engines that had indexed the Tuia 250 site.

The configuration of access to the media library for search indexing bots is consistent with websites that are constructed for maximum visibility, promotion and distribution of information from the site as widely as possible. They are appropriate for these purposes. This was the original purpose of the Tuia 250 website.

These settings are inappropriate for sites that are collecting and storing personal information from users of the website at least in respect of folders where that information is to be stored. There was no dispute by anyone we spoke with about this lack of security for personal information.

Some applications received by MCH using means other than the online application process were uploaded to the Tuia 250 website using the application webform by MCH staff. Obviously, this was done in the belief that personal information was being securely managed.

On 22 August, MCH received notification from a person about a breach of personal information an individual had supplied to MCH as part of their application for the Tuia Trainee Programme. MCH responded to the breach immediately[5] and the Tuia 250 website, including the Tuia Trainee Programme online application process, was taken down.

It is important to state that the above comments relate only to documents containing personal information that were uploaded as part of the application process. These comments do not relate to personal information collected in the course of completing the

[2] It is to be noted that we were not able to determine exactly that this was the case. It seems to us however, to be the most likely cause of the breach.
[3] Again, we consider this the most likely scenario. However, because event logs were not available this cannot be conclusively verified.
4 Note because event logs were only kept for 5 days it is not possible to say definitively that this was the case. The Supplier contends that settings could have been changed by MCH during the realignment of the website by MCH when they had total control of the site. MCH staff told us that these were server controls and that they would not have had access to these. They also said that because the Supplier had provided assurances as to the site's security settings, they had no need to change settings even if they could have.
[5] Note: how MCH responded is outside the terms of this review.

form itself because this information was not breached.

In our view issues are raised in terms of the management of personal information under the following principles of the *Privacy Act 1993*:

- **Principle 1 – Purpose of Collection of Personal Information**. Collection of personal information is necessary to assess applications for a place on the Tuia Trainee Programme. In our view there is an available interpretation that more information was collected than was required to make this decision. Identity documents were not necessary to make this decision and could have been sought from successful applicants after the decision on the application had been made[6]. We do note however that MCH was working within tight timeframes and made an assessment that collecting this information was a reasonable business processing decision. However, had they only required identity information from successful applicants the number of individuals affected by the breach would have reduced to only those that were successful in their applications. In hindsight we consider there were viable alternatives that might have been deployed that could still have met MCH's timeframes.
- **Principle 5 - Storage and security of personal information**. This principle requires that information is protected by;

  > *such security safeguards as it is reasonable in the circumstances to take, against…access, use, modification, or disclosure, except with the authority of the agency that holds the information and other misuse and that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information*.

  In this case the information was not sufficiently protected because it could be accessed and used when stored on the Tuia 250 website.
- **Principle 9 – Agency not to keep personal information for longer than necessary**. An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used. This storage limitation provision may also have been breached. This is because personal information was kept after the decision on an application had been made. While this would not have prevented the breach in that the personal information would have been insecure for the time it was held on the website, it was exposed for a longer period of time due to not removing the personal information after the decision had been made (in respect of unsuccessful applicants at least). There is a question as to the necessity of storing the information in the media library of the website rather than transferring it to MCH held IT infrastructure after collection.

***Mandatory protective security requirements***

As well as issues relating to operating outside of the principles of the Privacy Act, MCH was not compliant with some of government's mandatory protective security requirements (PSR).[7]

In particular the requirements to:

- *Design security measures that address the risks your organisation faces and are consistent with your risk appetite. Your security measures must be in line with:*
  *•……*
  *• any privacy, legal, and regulatory obligations that you operate under.*

[6] See the PADLOCK assessment information available from the Office of the Privacy Commissioner at: https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/PADLOCK-DL-brochure-for-web-Aug-2017.pdf
[7] https://www.protectivesecurity.govt.nz/about-the-psr/mandatory-requirements/

- *Confirm that your information security measures have been correctly implemented and are fit for purpose.*
- *Complete the certification and accreditation process to ensure your ICT systems have approval to operate.*

***Identification and management of risks regarding management of personal information***

The RSG risk identification in relation to personal information can be summarised as "*Trainee Crew processes in design, key risks around safety and coordination*". We are not aware of anything that would suggest that the security of personal information collected through the Tuia Trainee Programme was specifically considered as an independent risk to be mitigated within the Tuia 250 project.

On or about 15 May 2019, MCH staff associated with implementing the decision to use the webform for Tuia Trainee Programme met. This process identified risks associated with the Tuia Trainee Programme and other issues associated with the wider Tuia 250 project.

In addition to meetings and discussions, information management plans were prepared and added to during the course of the project.[8] The following relevant risks were identified and proposals to manage those risks made in relation to personal information connected with the Tuia Trainee Programme online application before the webform went live on the Tuia 250 website:

- *Staff, contractors and others involved may not have a sufficiently developed understanding of the requirements for handling personal information in the Privacy Act 1993 and the importance of maintaining public trust in the handling of their personal information by agencies.*
- *Although a supplier was engaged by MCH to manage the Tuia Trainee Programme online application process, responsibility for the protection of personal information remains that of MCH.*
- *If a contractor is engaged to gather, store and provide this information to MCH in the form requested, MCH must assess the processes and policies of the Supplier regarding privacy, iterating in agreements the location and method of storage, security, and disposal once the information has been collected.*
- *Establish an email application process to provide security.*
- *Business systems pose potential risk of breach of information. Management decisions must be made to mitigate risk as much as practical and possible.*
- *MCH providing advice and guidance to help ensure steps are taken to protect personal information in the event of a breach.*

In addition to identifying these risks, a series of action points were also developed and responsibility for carrying them out allocated to relevant staff at MCH. The action points were designed to provide assurance that the risks which had been identified were being mitigated.

The internal process was also supplemented with external advice. Specifically, general advice was sought and received from the Office of the Government Chief Privacy Officer about the proposed process. This helped to formulate the risks identified above, and the steps to be taken in respect of those risks.

In our view, the only risk not identified was the risk related to collecting personal information relating to identity and age at the application stage from all applicants and not that the stage when applicants had been advised they had been successful in applying for a trainee crew position. While it was not strictly necessary for the purpose of assessing eligibility for the Tuia Trainee Programme, we understand this was a pragmatic decision given the tight timeframes MCH were working to. Nevertheless, we did not see any evaluation of alternatives to

[8] Noting that information management plans were still being written after the webform had gone live.

streamlining the process that could have been used which did not require the uploading of identity/proof of age documents[9]. Not identifying this risk and not considering alternative approaches, contributed to the breach affecting more people than it otherwise would have.

The collection of personal information comes with a consequential risk of a breach with respect to that information. The principle of 'collection limitation' serves to reduce both the occurrence and severity or extent of potential breaches. In designing programmes, processes and systems, this principle should always be considered to determine if the goal can be achieved without collecting personal information, or any more personal information than is strictly required. In this case the webform used required and reminded applicants to attach files that were evidence of their identity. The breach relates mostly to this information. Also, MCH staff uploaded some identification documents to the Tuia 250 website themselves. This material was also part of the breach.

MCH has a Privacy Officer, however this is not a full-time role and is one of a number of roles that this individual performs. This is not unusual for a small agency. The role is situated in the IT team within MCH. It is not situated in the legal team of MCH even though often a Privacy Officer will be required to advise on compliance with legislation, namely the *Privacy Act 1993* as well as other regulations and obligations including All-of-Government rules such as the PSR.

We make no criticism of the Privacy Officer in this regard, nor of the work performed that we have seen in this review. We do consider there is merit in MCH considering having the Privacy Officer role located within its legal team however for the reasons outlined above.

Email correspondence and documentation of MCH records that Information Management planning was being undertaken while the Tuia Trainee Programme application process was underway. In effect, this meant that files attached to applications made using the webform were being assessed for information management purposes while collection of that personal information, and in this case the breach, was already occurring. This is not best practice. Information management processes should be completed before personal information is collected. This is also not consistent with a privacy by design approach.

More broadly than the Tuia 250 website, MCH completed the GCPO Privacy Self-Assessment 2018-2019 risk assessment section and self-reported a level 2 rating for risk assessment in relation to privacy matters. A level 2 rating means:

- *Incomplete or underdeveloped processes for privacy risk identification. Privacy risk management is issues-based.*
- *Regular or occasional risk identification and assessment is performed.*
- *Privacy risks are monitored on a siloed basis in business lines, with little if any cross-functional interaction.*
- *Privacy risk reporting is largely by exception and in response to identified issues.*

MCH's comments in relation to this section were "*We remain at the current level and target of 2. This level is appropriate for our risk profile, our use of personal information, information systems and business outputs*".

This level of privacy risk assessment seems appropriate for the normal routine work of MCH. In our view it is not an adequate assessment level for a Ministry involved in the collection of personal information in the manner envisaged by the Tuia Trainee Programme where a greater level of privacy risk assessment and management was needed.

[9] For e.g. using a declaration on the application form (which would make applicants subject to the requirements of the Oaths and Declarations Act 1957), or on the basis that if successful applicants would submit proof of identify and age within a specified period.

## 8. Timeline of the breach

The timeline of the breach is attached (Appendix 3).

## 9. Whether the Ministry adhered to internal policies, applicable government policies and good practice guidelines

MCH broadly adhered to its internal and government policies and good practice guidelines in respect of the procurement process for the Tuia 250 website. It did not properly reflect contractual variations formally in documentation recording the agreement between the parties.

MCH did not adhere to internal and government policies and good practice guidelines in respect of the collection and management of personal information, including risk identification.

Specifically, MCH:

- Was not fully compliant with the requirements of the Privacy Act. While we understand that there was a need to reduce the time between applications for the Tuia Trainee Programme being received and being able to advise successful applicants, collecting identity information from all applicants is inconsistent with the principles of the Privacy Act. It was not necessary to have formal proof of identity in order to determine trainee voyage crew member applications. Applications could have been decided on using either a declaration on the application form[10], or on the basis that successful applicants would be required to submit proof of identify and age within a specified period or their application would lapse.
- Did not protect the personal information against access or disclosure with reasonable security safeguards. The information was collected for the agency by the Supplier in connection with the provision of a service to the agency, and everything reasonably within the power of the agency was not done to prevent unauthorised use or disclosure of that information. We believe that a reasonable safeguard would have been to have tested the website to provide positive assurance that personal information held on the site was secure prior to going live with the webform. Notwithstanding the error was likely caused by the Supplier having the incorrect security settings on the files containing personal information, MCH remains accountable for the proper management of personal information. In this regard we consider MCH to be in the same position as other government agencies that collect, store and use personal information. We reviewed the Ministry's web guidelines. We also reviewed the guidelines of the GCDO and GCISO mandatory PSR standards and guidelines and spoke with a number of staff from the GCDO. While there appears to be no specific mandatory directive that would have required MCH to undertake positive penetration testing of the security settings of the folders prior to the website going live, we consider that taken together, the clear intent of the standards and guidelines is that appropriate security settings are required to be in place and that these should be tested.[11] Agency Chief Executives are ultimately accountable for ensuring their agencies are compliant with these requirements in the same way there are accountable for compliance with the law, government policy and other standards and guidance.
- Stored personal information for longer than was needed.[12] Personal information was retained on the website after decisions about applications had been made. Once

[10] Which would have made applicants subject to the requirements of the Oaths and Declarations Act 1957.
[11] For e.g. PSR mandatory requirement INFOSEC 3 provides: Confirm that your information security measures have been correctly implemented and are fit for purpose
[12] We note that government agencies have obligations under the Public Records Act which may create certain obligations that need to be rationalised with their obligations under the Privacy Act

these decisions had been made, this information or any of the information that was no longer required should have been securely disposed of. While the breach would have still occurred, the duration of the breach would have been reduced. Applications closed on 26 June 2019. The breach was not discovered until 22 August 2019, almost 2 months later. At that time the information was still held on all applicants and stored in the same insecure place. Additionally, the contract with the Supplier, although it did not require the online trainee application process, did require a complete copy of the site to be provided to MCH at the conclusion of the contract. This would, on the face of it, include any personal information collected and therefore that would be required to be copied and stored at this point also.

- Was still completing information management plans after personal information was already being stored insecurely and while a breach was occurring, albeit this was unknown to MCH. This is not best practice and these plans should be completed and implemented before personal information is collected, used and stored.
- Was not compliant with some of government's mandatory protective security requirements (PSR).[13] In particular the requirements to:
    - Design security measures that address the risks your organisation faces and are consistent with your risk appetite. Your security measures must be in line with:
      •……any privacy, legal, and regulatory obligations that you operate under.
    - Confirm that your information security measures have been correctly implemented and are fit for purpose.
    - Complete the certification and accreditation process to ensure your ICT systems have approval to operate.

# Findings and Recommendations

## 10. Findings

As a result of our review of the documents, the research we undertook and the interviews we conducted, we make the following findings:

***Procurement processes and probity***

1. That the Supplier of the services to construct the Tuia 250 website and an MCH staff member had a professional association that pre-dated the procurement process. This association, whilst known by some MCH staff and management, was not formally declared, although the staff member believes they raised it appropriately with management at the start of the procurement process.
2. The MCH staff member believed the Supplier would be suitable for providing the Tuia 250 website because of a number of factors. These included, but were not limited to, their understanding of the previous work the Supplier had undertaken with voyaging and the associated kaupapa, their ability to provide content in multiple relevant languages and their previous experience of working with the Supplier.
3. The MCH staff member provided assistance to the Supplier in the course of them submitting their proposal. While permissible, best practice would have been to make the same assistance available to other interested suppliers.
4. Because of the MCH staff member's association with one potential supplier MCH took steps to ensure that staff member did not take any further part in the

[13] https://www.protectivesecurity.govt.nz/about-the-psr/mandatory-requirements/

procurement process.

5. A five-member procurement panel was formed (three core and two technical advisors). Proposals from two other suppliers were considered as part of this procurement process. Following the panel's assessment, the Supplier was awarded the contract to build and host the Tuia 250 website using a third-party hosting service.

6. The contract specified the deliverables for the build and functionality of the website. This did not include providing any functionality for managing applications for trainees because at that stage MCH did not know how it was going to manage that aspect of the Tuia 250 programme.

***The design and construction of the website***

7. Given MCH's requirements, the Tuia 250 website was designed to provide as much information stored on the site as possible. This was consistent with the purpose and objectives of the website i.e. to provide anyone searching for information about the Tuia 250 Encounters programme with as much information about the programme as possible. Technically this was facilitated by allowing as much of the content as possible to be *indexed* and therefore able to be accessed by search engines when the site went live.

8. The initial development of the website and content did not meet the Ministry's requirements and additional support was given to the Supplier by MCH staff including from its web team. To facilitate this, administrative access to the site was provided to MCH by the Supplier. This allowed MCH staff to load content directly onto the site and to change the look and feel of the site to better meet MCH's requirements.

***Managing applications for the Tuia Trainee Programme***

9. In May 2019 the decision was made by MCH to use the website to help manage applications for the Tuia Trainee Programme. This decision does not appear to have been made as part of any formal steering or governance arrangement and was taken by the Deputy Chief Executive - Tuia 250. It was not formally recorded and does not appear to have been risk assessed. The Supplier agreed that they could host a webform on the website.

10. A new section was added to the website for this purpose. This section of the site was intended to collect application details including personal information from trainees. This was fundamentally a different purpose from what was originally required by MCH. The information collected would need to be securely stored for later access and use by MCH.

11. MCH and the Supplier agreed that the Supplier would provide the Tuia Trainee Programme online application process on the Tuia 250 website.

12. There was no formal variation of the contract between MCH and the Supplier recording that the Supplier would provide the Tuia Trainee Programme online application process. In part this was because one of the deliverables under the original contract was no longer required, meaning there was scope within the budget and because hosting the webform was a relatively straightforward process.

***Security concerns and the data/personal information breach***

13. In June 2019 there were ongoing concerns about the quality of the design of the Tuia 250 website as well as concerns over the security of the CMS and website generally. One of the concerns raised was that personal information was viewable in the media library on the website. While this was only viewable to someone with administrative rights to the website, there was a concern expressed within MCH that this raised a

risk that personal information could inadvertently be *published* onto the website.

14. These concerns led to the Tuia Trainee Programme section of the Tuia 250 website being taken down between 8 and 12 June 2019.
15. The site was reinstated following the provision of assurances from the Supplier about the security of the CMS, website and server. Assurances around the management of personal information were also obtained from within MCH. The assurances provided to MCH included the statement that the personal information that was the subject of the breach was not encrypted on the server, however industry standard security was in place which would prevent unauthorised access to personal information.
16. Unknown to the Supplier and MCH at this time was that the personal information collected through the webform on the website had most probably already been indexed by search bots and quite possibly already been accessed more than once.
17. The breach was not caused by the CMS used by the Supplier of the Tuia 250 website.
18. The breach was not caused by hacking or the action of an external party.
19. The breach was most likely caused by an incorrect file configuration allowing access to files uploaded to the site including those relating to online applications for the Tuia Trainee Programme. Files uploaded as part of applications were stored in the media library of the Tuia 250 website.
20. All files in the media library including those containing the personal information of applicants for trainee positions were available for indexing by search engines.
21. Once indexed, the personal information would be returned in search results for properly configured search requests made using search engines that had indexed the files. We were advised that sophisticated search engines like Google and BING would most probably have indexed the files containing the personal information within 2 days of the material being uploaded and then on an ongoing basis, as that is what they are designed to do.
22. This is precisely what *brochure websites* are intended to have happen to them as this makes the information on the website easy to search for and access.
23. The breach is therefore most likely to have begun shortly after the first application was uploaded using the Tuia Trainee Programme online application form after it went live on 28 May 2019.
24. The breach continued (with the exception of the period where the website was taken down and then reinstated in June 2019) until the website was permanently taken down on 22 August 2019.
25. Using the website for the management of personal information was not considered as part of the risk assessment processes for the website because initially this was not in scope. It was not reconsidered as part of the wider Tuia 250 risk management processes when the scope was subsequently changed.
26. The lack of more formal and structured governance arrangements overseeing the planning and delivery of the Tuia 250 program, including the voyage trainee component of the program, we believe contributed to a loss of visibility and management oversight of risks. This led to decisions being made without full information and proper consideration of all the options and risks.
27. While MCH quite properly identified the risks relating to the collection of personal information as part of its information risk management assessment, this did not translate into an appropriate level of testing of the Tuia Trainee Programme online

application process, including testing of the website itself, to determine if it was in fact, secure and appropriately configured for the storage of personal information.

28. No privacy impact assessment was done, although the information risk management assessment noted a breach of privacy as a key risk.
29. The processes used by the Ministry and the Supplier did not meet best practice risk management, Privacy Act or government protective security requirements.
30. The assumption made by both the Supplier and MCH was that the security settings in place to prevent unauthorised access to the site also meant that information on the site with respect to trainees' applications for crew positions was stored securely. Clearly it was not and most probably it never was.
31. Believing the website and personal information on it was secure, MCH staff also uploaded personal information relating to some applications received by MCH through other means e.g. email direct to MCH. This personal information was also stored in the media library and was also insecure and was probably indexed and searchable shortly after it was uploaded.
32. The webform deployed by MCH required applicants to upload attachments to their application to establish their identity and their date of birth. It is these identity documents that form the bulk of the personal information that was compromised. Other personal information entered into the form, as opposed to being attached to it, was stored elsewhere and not part of the breach.
33. Compounding the breach was the decision taken to require the uploading of identity and proof of age documents at the time of making an application, rather than after an applicant had been be advised their application had been successful. While we understand that this was a pragmatic decision given the need to reduce the time between application and being able to advise successful applicants, this was inconsistent with the requirements of the Privacy Act to only collect as much personal information as was necessary for the purpose of determining applications in the first instance.
34. Whilst out of scope, we note that following the discovery of the breach the Ministry acted promptly and appropriately to inform applicants, the Privacy Commissioner and other appropriate agencies. MCH immediately took the site down and it is now currently hosted by the Ministry.

## 11. Recommendations

Having regard to our findings we make the following recommendations:

1. MCH review its procurement systems and processes, the application of whole of government procurement practices and necessary internal processes for approving the engagement of services outside of this process. This should include training around variations of contracts with suppliers, the engagement of the legal team within MCH in connection with contracts with suppliers, the management of interests in the procurement process and what constitutes appropriate assistance during an RFP process. Information retention and records management best practice and procedures in procurement should also be reviewed and ensured are included in training and requirements of MCH.
2. MCH management review induction materials and training and update these to ensure they have best practice approaches concerning the identification, declaration and management of conflicts of interest between staff and suppliers in the procurement process. This should include training on the types of appropriate assistance staff may provide to prospective suppliers during a procurement process. Training should also include the requirement that people document their interactions

with potential suppliers during a procurement process and that these are disclosed to people within the Ministry with responsibility for the fair and impartial conduct of government procurement processes.

3. MCH ensure that prior to its collection, storage and use of personal information it undertakes and documents a risk assessment and that this includes evaluating the integrity of the systems it proposes to use to ensure they are appropriate and operating as intended. This should include positive penetration testing prior to any system going live, when any changes are made and in any case at regular intervals.
4. MCH review its internal privacy policies and practices and adopt mandatory privacy impact assessments on any project that involves personal information and require these, and any other management plans relating to that information to be completed before collecting any personal information or implementing any plans or projects requiring the collection of personal information. Implementation of Privacy by Design practices and procedures would benefit MCH in future whenever it is collecting personal information.
5. MCH review its policies to require that its Privacy Officer is formally allocated to any project where MCH is dealing with personal information at the earliest possible stage to ensure that privacy risks are identified, managed and mitigated against from the earliest possible opportunity.
6. MCH consider aligning the Privacy Officer role to its legal services function. This is a conventional structural alignment in other agencies. Information management and the security of information management systems are related functions that can be aligned within the information management function of the Ministry.
7. MCH consider the appropriateness of contractual terms that require entire copies of websites to be provided by a supplier at the conclusion of the contract where those websites hold personal information. Such clauses may result in storage of personal information beyond the time period for which it is required and allow for that information to be used for purposes other than those for which it was collected. We recommend that personal information be considered for exclusion from such provisions.
8. MCH review its internal governance arrangements to ensure it leverages the skills and experience it has available across all parts of its operations as appropriate. As a small agency, establishing governance arrangements from within teams and programmes is never likely to be able to assemble the necessary skills and experience to operate effective governance. Taking a Ministry-wide approach, and where appropriate supplementation from outside the agency, is more likely to equip the Ministry to build fit for purpose governance structures.
9. MCH consider the findings of this Review and, in line with the Terms of Reference, share this report with the Government Chief Digital Officer, the Government Chief Information Security Officer and the State Services Commission.

## 12. Next Steps

We consider that the next steps are:

- Consider and provide any feedback on this report as to factual inaccuracy or missing information.

- Discuss our findings and recommendations internally and with relevant external agencies and consider the implications of implementing our recommendations, including recommendation 3.

# Appendix 1

## List of People Interviewed

- Bernadette Cavanagh, Chief Executive, Manatū Taonga, Ministry for Culture and Heritage
- Paul James, Chief Executive and Government Chief Digital Officer, Te Tari Taiwhenua, Department of Internal Affairs
- Renee Graham, Chief Executive, Minititanga mō ngā Wāhine, Ministry for Women,
- Russell Cooke, Government Chief Privacy Officer, Te Tari Taiwhenua, Department of Internal Affairs
- Chris Blackford, Account Executive, Government Chief Digital Office, Te Tari Taiwhenua, Department of Internal Affairs
- Becky MacNeill, Deputy Chief Executive Organisational Performance & Delivery, Manatū Taonga, Ministry for Culture and Heritage
- Tamsin Evans, Deputy Chief Executive Tuia 250, Manatū Taonga, Ministry for Culture and Heritage
- Aaron Lloyd, Chief Legal Advisor, Manatū Taonga, Ministry for Culture and Heritage
- Brendan Booth, Chief Legal Advisor, Te Manatū Waka, Ministry of Transport
- Manager Finance and Strategic Planning, Manatū Taonga, Ministry for Culture and Heritage
- Chief Information Officer, Manatū Taonga, Ministry for Culture and Heritage
- Manager, Production Research & Publishing, Manatū Taonga, Ministry for Culture and Heritage
- Senior Advisor, Government Chief Privacy Office, Te Tari Taiwhenua, Department of Internal Affairs
- Senior Advisor – Tuia 250, Manatū Taonga, Ministry for Culture and Heritage
- Manager Communications & Ministerial Services, Manatū Taonga, Ministry for Culture and Heritage
- General Manager, System Assurance, Te Tari Taiwhenua, Department of Internal Affairs
- Technical Development Lead – Production Research & Publishing, Manatū Taonga, Ministry for Culture and Heritage
- Privacy Officer, Manatū Taonga, Ministry for Culture and Heritage
- Project Manager – Voyaging Tuia 25, via email, Manatū Taonga, Ministry for Culture and Heritage
- Project Director - Tuia 250, Manatū Taonga, Ministry for Culture and Heritage
- The Supplier

# Appendix 2

30 August 2019

## Terms of reference for an independent review of the Tuia 250 voyage trainee privacy breach

The Chief Executive of the Ministry for Culture and Heritage has commissioned an independent Review of the Ministry's decisions and processes relating to:

- the circumstances that led to the breach of applicants' personal information, and
- procurement and management of the Tuia 250 website (https://www.tuia250.nz/) used to receive applications for the Tuia 250 trainee crew programme.

The review will be led by Doug Craig, director of The RDC Group Limited.

## Context

The Ministry is leading the *Tuia - Encounters 250* national commemoration. This is a programme of events, education and reflection that celebrates Aotearoa New Zealand's Pacific voyaging heritage and acknowledges the first onshore encounters between Māori and Pākehā in 1769–70.

The Voyage Trainee programme gives New Zealanders the opportunity to sail aboard the vessels in the Tuia 250 *Voyage* during October to December 2019.

A privacy breach has occurred whereby the personal details of people who applied to the Tuia 250 *Voyage* trainee crew programme have been compromised. The private data includes images of passports, driver's licences, birth certificates and other forms of identification stored on the Tuia 250 website.

## Objectives of the review

The objectives of the independent review are to:

- build a comprehensive understanding of the situation and cause of the privacy breach
- inform the Ministry to prevent such a situation occurring again.

## Matters in scope of this review

The review will make findings about the facts, provide an analysis to determine what caused the breach, identify lessons learned and make recommendations to the Chief Executive on changes and improvements needed to avoid a similar breach in the future.

In particular, the review will investigate:

- the governance and management of the Tuia 250 Voyage trainee crew programme, relating to:
    - the decision to use an externally built and hosted website to receive applications for trainee crew members
    - the management of personal information
    - identification and management of risks regarding management of personal information
- The procurement process, including:
    - analysis of technical requirements
    - analysis of potential Supplier proposals
    - selection of the preferred Supplier
    - contractual arrangements between the Ministry and the Supplier including the brief, agreed technical specifications, and variations to create the online application function
    - management of the contract and relationship with the Supplier throughout the duration of the work
- The Tuia 250 website (https://www.tuia250.nz/) itself, in particular technical functionality with respect to information security and management of personal information
- The timeline of the breach, including when and how it was identified by the Ministry
- Whether the Ministry adhered to its internal policies and to applicable government policies and good practice guidance.

## Matters out of scope of this review

- The governance and management of the wider Tuia 250 programme, to the extent that this can be separated from the governance and management of the trainee crew programme
- The Ministry's main website or other digital assets
- The response to the privacy breach itself, once the Ministry became aware of it (this will be the subject of a separate debrief)
- Third party actions arising from the breach, such as unauthorised use of personal information
- Conduct or professional performance of individual staff members

## Deliverables, timeframes and reporting

The review must be carried out urgently, with an indicative date for the final report of 18 October 2019. The reviewer will give regular oral progress reports to the Chief Executive.

The final review report will be delivered to the Chief Executive. The Chief Executive will provide a copy to the Government Chief Digital Officer, the Government Chief Information Security Officer, and the State Services Commissioner.

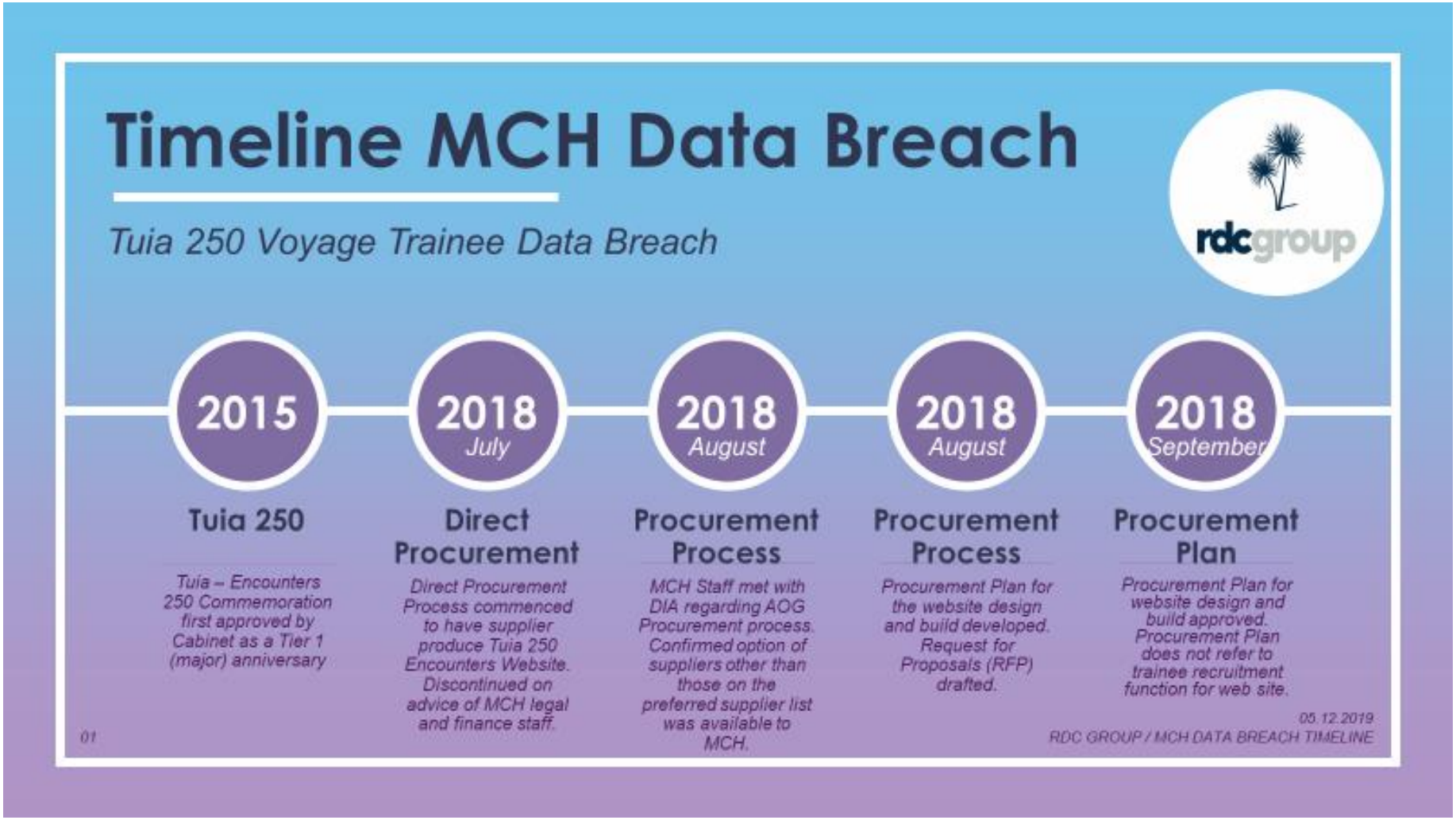
The final report will be publicly released by the Ministry as soon as practicable.

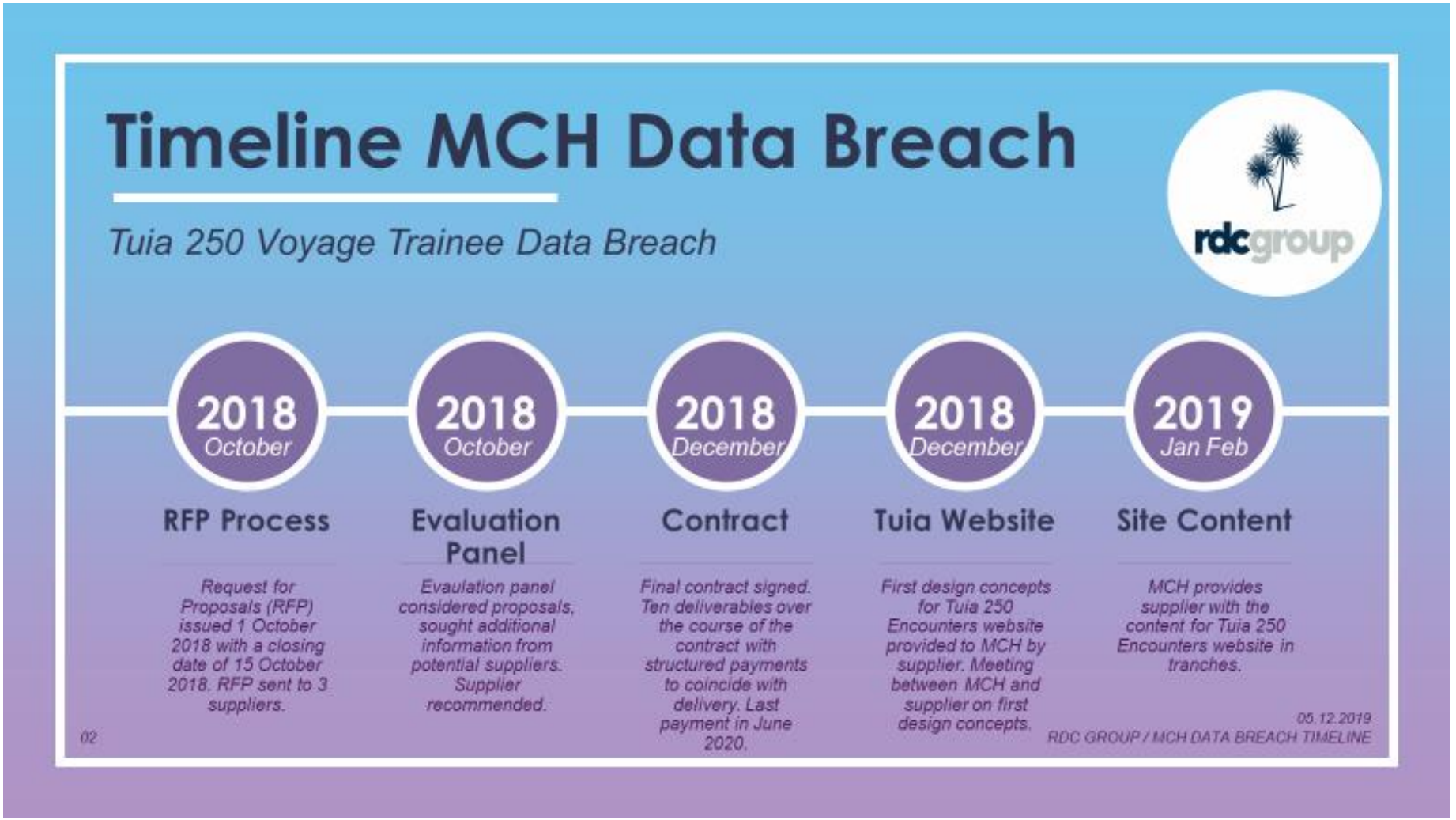
---

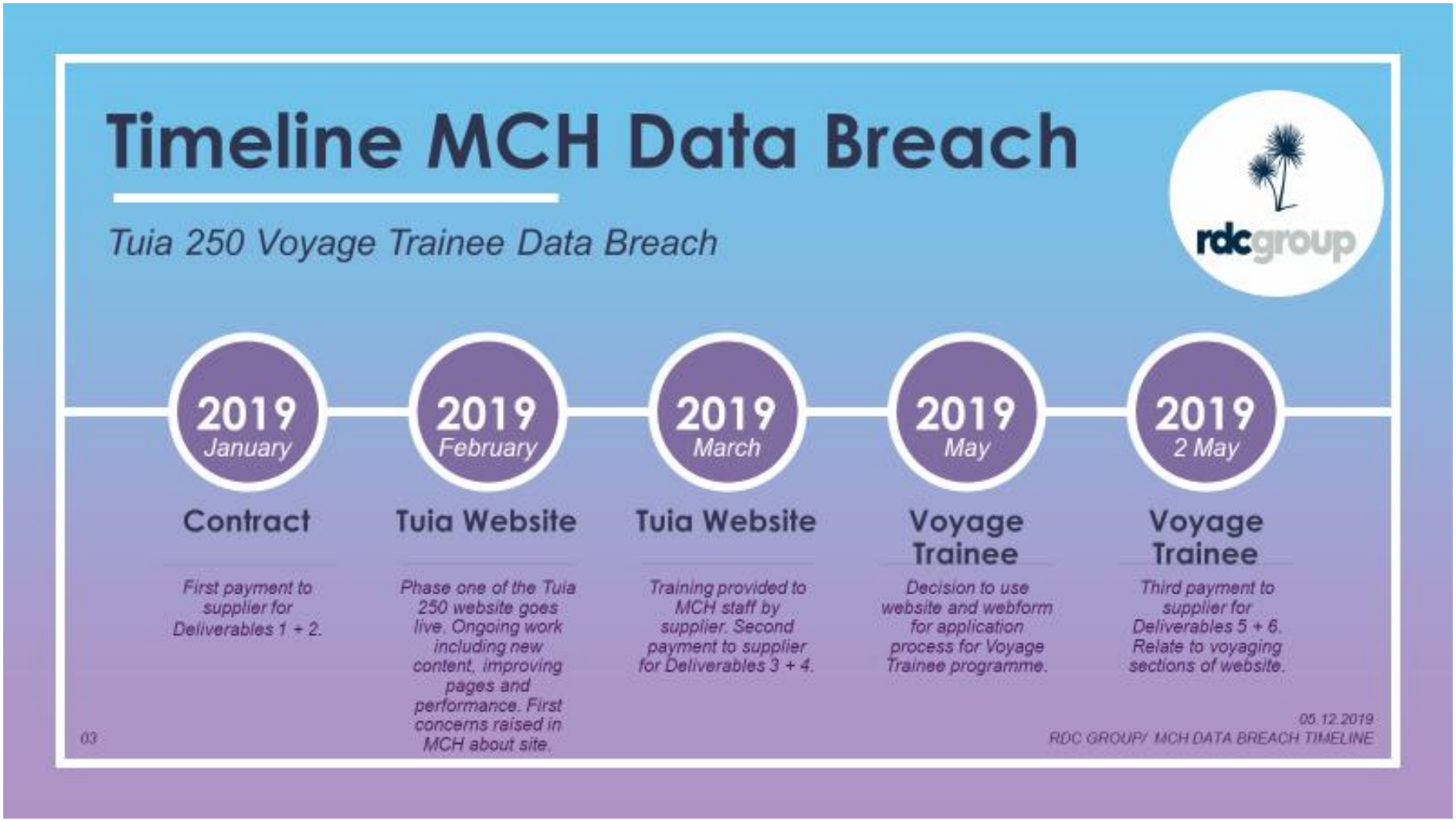
Bernadette Cavanagh Date 30 August 2019

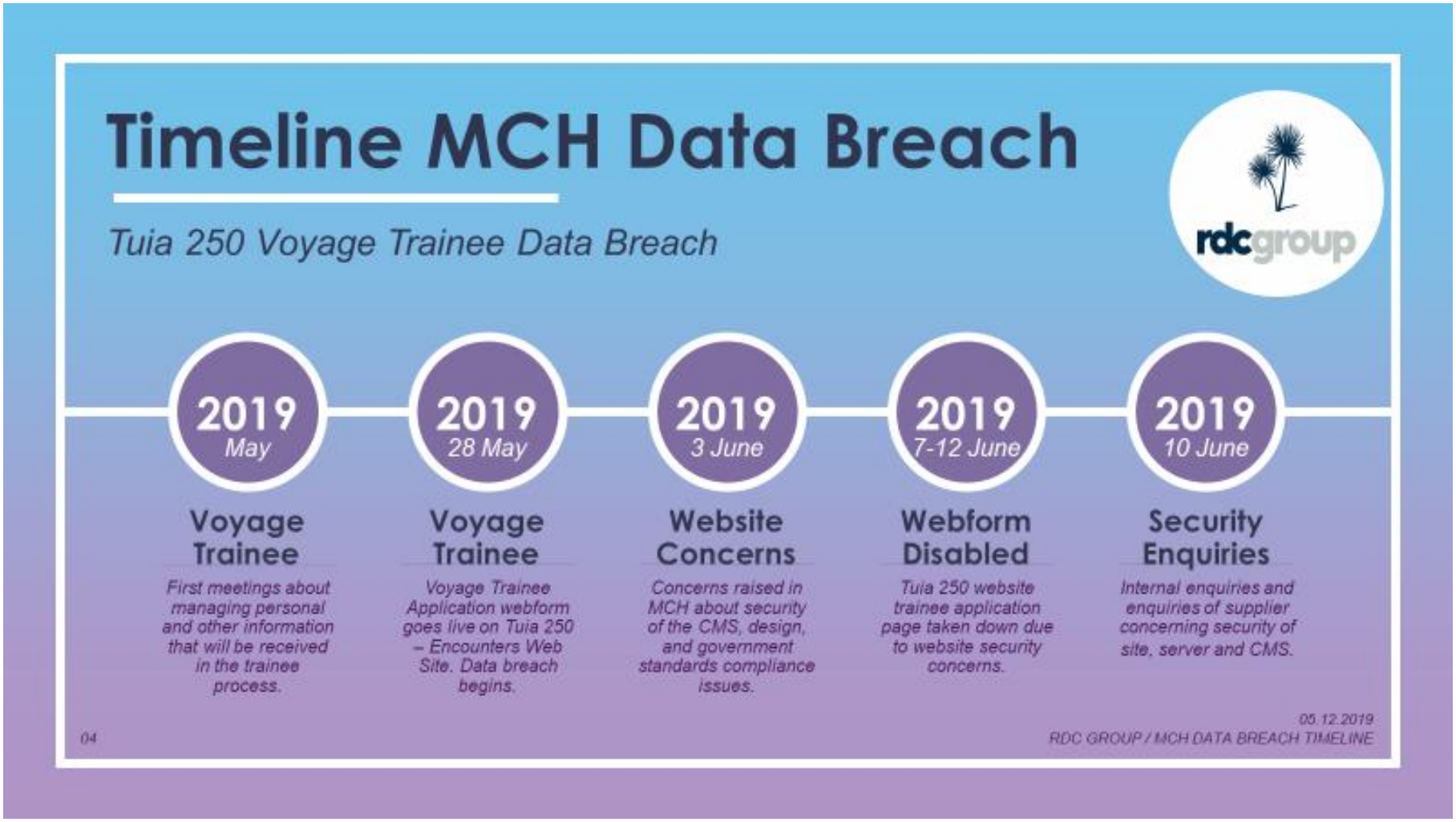
Chief Executive

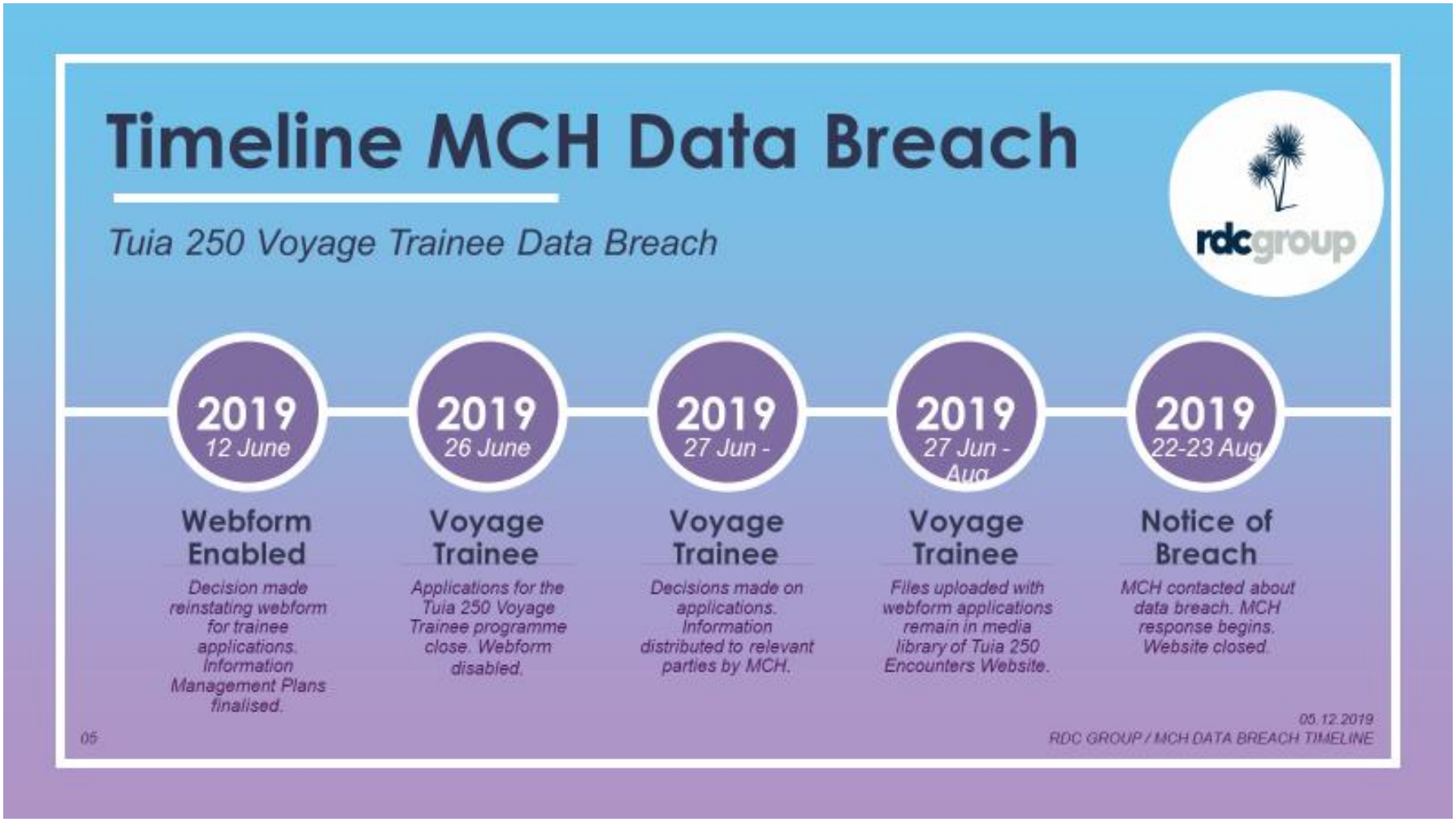
## Appendix 3




Timeline MCH Data Breach
Tuia 250 Voyage Trainee Data Breach
rdcgroup
2018 October
RFP Process
Request for Proposals (RFP) issued 1 October 2018 with a closing date of 15 October 2018. RFP sent to 3 suppliers.
2018 October
Evaluation Panel
Evaulation panel considered proposals, sought additional information from potential suppliers. Supplier recommended.
2018 December
Contract
Final contract signed. Ten deliverables over the course of the contract with structured payments to coincide with delivery. Last payment in June 2020.
2018 December
Tuia Website
First design concepts for Tuia 250 Encounters website provided to MCH by supplier. Meeting between MCH and supplier on first design concepts.
2019 Jan Feb
Site Content
MCH provides supplier with the content for Tuia 250 Encounters website in tranches.
02
05.12.2019
RDC GROUP / MCH DATA BREACH TIMELINE


Timeline MCH Data Breach
Tuia 250 Voyage Trainee Data Breach
rdcgroup
2019 January
Contract
First payment to supplier for Deliverables 1 + 2.
2019 February
Tuia Website
Phase one of the Tuia 250 website goes live. Ongoing work including new content, improving pages and performance. First concerns raised in MCH about site.
2019 March
Tuia Website
Training provided to MCH staff by supplier. Second payment to supplier for Deliverables 3 + 4.
2019 May
Voyage Trainee
Decision to use website and webform for application process for Voyage Trainee programme.
2019 2 May
Voyage Trainee
Third payment to supplier for Deliverables 5 + 6. Relate to voyaging sections of website.
03
05.12.2019
RDC GROUP/ MCH DATA BREACH TIMELINE


Timeline MCH Data Breach
Tuia 250 Voyage Trainee Data Breach
rdcgroup
2019 May
Voyage Trainee
First meetings about managing personal and other information that will be received in the trainee process.
2019 28 May
Voyage Trainee
Voyage Trainee Application webform goes live on Tuia 250 – Encounters Web Site. Data breach begins.
2019 3 June
Website Concerns
Concerns raised in MCH about security of the CMS, design, and government standards compliance issues.
2019 7-12 June
Webform Disabled
Tuia 250 website trainee application page taken down due to website security concerns.
2019 10 June
Security Enquiries
Internal enquiries and enquiries of supplier concerning security of site, server and CMS.
04
05.12.2019
RDC GROUP / MCH DATA BREACH TIMELINE


Timeline MCH Data Breach
Tuia 250 Voyage Trainee Data Breach
rdcgroup
2019
12 June
Webform Enabled
Decision made reinstating webform for trainee applications. Information Management Plans finalised.
2019
26 June
Voyage Trainee
Applications for the Tuia 250 Voyage Trainee programme close. Webform disabled.
2019
27 Jun -
Voyage Trainee
Decisions made on applications. Information distributed to relevant parties by MCH.
2019
27 Jun - Aug
Voyage Trainee
Files uploaded with webform applications remain in media library of Tuia 250 Encounters Website.
2019
22-23 Aug
Notice of Breach
MCH contacted about data breach. MCH response begins. Website closed.
05
05.12.2019
RDC GROUP / MCH DATA BREACH TIMELINE