Manatū Taonga
Ministry for Culture & Heritage

Ministry response to the Tuia 250 Voyage Trainee Privacy Breach Independent Review

18 December 2019

Contents

1. Background

On 30 August 2019, the Chief Executive of Manatū Taonga, the Ministry for Culture and Heritage, commissioned an independent review of the Ministry'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.

The review was undertaken by Doug Craig of The RDC Group Ltd. The final report was provided to the Chief Executive of the Ministry for Culture and Heritage on 5 December 2019. This document is in response to the Final Report of the Independent Review of the Tuia 250 Voyage Trainee Privacy Breach.

A full copy of the report is available from the Ministry's website, www.mch.govt.nz.

2. How will the Ministry respond immediately?

The Ministry accepts all recommendations in the report. Our immediate response will be to:

- Make penetration testing mandatory on all technical systems that hold personal information and commit to ensuring that no system will go live without this testing showing that personal information will be secure.
- Move the role of Privacy Officer to sit with the Chief Legal Adviser and ensure all new projects with privacy implications are appropriately managed through all stages of the project.
- Require that all systems that hold or are intended to hold personal information will require sign-off at Deputy Chief Executive level, after assurance from the Privacy and Chief Information Officers that the system has been assessed and tested to the appropriate level.

With these measures and other actions detailed in this response, the Ministry is confident a breach like the one that occurred with the Tuia 250 Voyage Trainee application process would have been prevented. The Ministry is committed to learning from the mistakes of this breach and ensuring that a situation like this does not occur again.

3. Review recommendations

The following provides the full text of all recommendations and the Ministry's response to each in brief. Our full discussion of the recommendations is addressed by theme in the following section, 'Our response to the recommendations'.

Recommendation 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.*

The Ministry commenced a refresh of its procurement management, processes and training earlier this year and will ensure that lessons learned from the Tuia privacy breach are reflected in our updated processes.

Recommendation 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.*

The Ministry now ensures that all new staff are given appropriate training on procurement and managing conflicts of interest as part of their induction and will provide refresher training for staff undertaking procurement for the first time or after a significant time period.

Recommendation 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.*

The Ministry will ensure that all systems – new and existing – that hold or are intended to hold personal information will be formally assessed for risk and penetration tested as recommended.

Recommendation 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.

The Ministry undertakes to review all policies as recommended and commits to adopting privacy by design practices and procedures.

Recommendation 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.

The Ministry will ensure that the Privacy Officer is formally allocated to projects that involve personal information and require that assurance is obtained from the Privacy Officer that appropriate assessments and actions have been followed before systems are released.

Recommendation 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.

The Ministry will assign the role of Privacy Officer to the Chief Legal Adviser and ensure ongoing close cooperation with information management processes and staff.

Recommendation 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.

The Ministry will ensure all contracts are appropriately drafted to ensure best practice and interpretation of the Privacy Act 1993, with particular regard to Principle 9 (Agency not to keep personal information for longer than necessary).

Recommendation 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.

The Ministry has begun immediate work to review its approach to governance to ensure it is in keeping with the risk profile of the agency and can expand and adapt as required by significant projects and programmes. This will include drawing on expertise from across the Ministry and wider system as appropriate.

Recommendation 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.

The Ministry is actively considering all findings and sharing them with the Government Chief Digital Officer, the Government Chief Information Security Officer and the State Services Commission.

4. Our response to the recommendations

This section provides a fuller discussion of how we are responding to the recommendations grouped around the themes of governance, procurement, privacy, and testing.

General comments

The Ministry fully accepts all findings and recommendations contained in the report, which provide a solid basis for improving the work and processes of the organisation.

The Ministry notes that the report finds our policies have generally been fit-for-purpose. However, in the case of the Tuia 250 Voyage Trainee programme, the policies were not well applied.

While out of scope of the review, the report notes that at times the Tuia 250 programme was under strain and acting quickly to deliver a significant work programme. This negatively affected the team's ability to give proper regard to policies and appropriate decision-making processes. Failings were also identified in the level of training provided to staff and general awareness of key Ministry policies and practices.

This does not excuse the Ministry's actions in failing to protect personal information. Rather, it points to areas for attention as the Ministry develops its processes for governing and managing programmes like Tuia 250 in future. The Ministry must adopt clearer guidelines for management and staff on role definition in relation to contract and supplier management, and the appropriate level of accountability and oversight of contractual relationships. Appropriate training across governance, procurement, privacy, and testing must be provided and adhered to by all staff in future.

The report raises some performance, training and capability issues, which will be worked through. It further points to the need to wrap better processes around our growing web and digital presence. The Ministry will need to focus on developing better processes and frameworks for governance, decision-making and accountability, risk identification and problem escalation, and personal information management.

Governance

To ensure effective governance, the Ministry will develop a governance framework that balances both the risk profile of the Ministry and the need to scale up for significant projects.

We fully agree with the report's recommendations in relation to work programme governance and will ensure that in future the range of skills and experience from across the organisation and system are drawn on. As noted above, the Ministry will also review how its web and digital presence is governed, including the appropriate location and recording of decision-making.

We note that the report identifies the risk profile of the Ministry as presenting specific challenges for governing programmes of Tuia 250's scale and complexity. The Ministry is developing a governance framework that takes account of the Ministry's risk profile but that can expand as required. This will necessitate drawing on relevant expertise from across the Ministry and wider system as appropriate. Other work programmes are already benefitting from increased attention to governance through dedicated funding for governance and programme management resource.

As part of this work, the Ministry will ensure projects and work programmes have clear lines of accountability and decision-making and problem/risk escalation processes. This work will give particular attention to large projects like Tuia 250 and the governance processes around our web and digital presence.

Procurement

For all contracts valued at over $25,000 (GST exclusive), the contract manager and budget manager (which must either be Deputy Chief Executive or Chief Executive level depending on the value of the contract) must currently sign the contract. As part of this process, advice must now be obtained from the Chief Legal Adviser and Chief Financial Officer in relation to the procurement process. Actions and decisions taken after that advice must be recorded by the relevant Deputy Chief Executive.

The Ministry has reviewed its procurement policy and procurement guidance for staff and has made enhancements to account for information retention and records management. These include a greater emphasis on due diligence, use of All-of Government panels, need for input from the Legal Team at earlier stages, and discipline about contract variation.

Ministry-wide training on procurement, including selection process, contract development, managing contract variations, and record keeping have all been identified by the Ministry's Legal Team as key areas for better training across the Ministry. The Ministry welcomes the report's findings and clarity for further action. This enhanced training is now underway and annual refresher training will be routine for all staff.

The Ministry's Legal Team has further developed more robust contractual terms regarding management of personal information. The new terms include stronger obligations to store information securely, discuss requests for information with the Ministry, and only use confidential or personal information for the purpose of the contract. Suppliers must also ensure all staff and subcontractors are aware of these obligations. The Ministry will ensure these are standard whenever services involve or require capture of personal information.

Privacy

To ensure proper adherence to our privacy policies, any system that holds or is intended to hold personal information will now require sign-off at Deputy Chief Executive level before it can be released for internal or external use. As

part of this process, advice must now be obtained from the Privacy Officer that the system has been appropriately assessed against Privacy Act requirements for the proper handling of personal information. Actions and decisions taken after that advice must be recorded by the relevant Deputy Chief Executive.

The Ministry is committed to improving its practices for managing and handling personal information and all recommendations in relation to privacy have been accepted. In particular, the Ministry commits to adopting 'privacy by design' and considering privacy impact assessments (PIAs) where necessary. These actions will enable the Privacy Officer to provide advice and guidance whenever personal information is proposed to be collected.

We agree that the Chief Legal Advisor be the designated Privacy Officer for the purpose of section 23 of the Privacy Act 1993, noting that this role has accountability for ensuring the statutory obligations are effectively discharged. We believe this is the single most important change we can make to ensure that where our work involves personal information, we are giving the right emphasis to looking after that information in accordance with the Act.

While the Ministry's privacy policy, guidance and framework is considered fit-for-purpose for an agency of its usual risk profile, they can be improved. In the case of the Tuia 250 Voyage Trainee application form, we did not follow our own policies. Training in this area will be included in staff induction alongside procurement training and will be required for all staff undertaking projects involving personal information.

We note that the Privacy Officer role needs to be resourced according to the demand on time required for carrying out the role and will ensure that both the information management and privacy elements of the role are considered. The Ministry will ensure that close cooperation between information management and legal functions within the Ministry are maintained and developed.

Testing

To ensure appropriate testing is undertaken, any system that holds or is intended to hold personal information will require sign-off at Deputy Chief Executive level before it can be released for internal or external use. As part of this process, advice must now be obtained from the Chief Information Officer that appropriate penetration testing has been undertaken and the system is secure. Actions and decisions taken after that advice must be recorded by the relevant Deputy Chief Executive.

The Ministry fully accepts the recommendation that we undertake appropriate testing of all public facing web services and where appropriate full penetration testing. Following the breach, the Ministry has undertaken full penetration testing of all external facing web services. No critical issues were found, and no personal information was able to be accessed. A number of minor recommendations were made to improve security, which we are currently implementing.

The Ministry has also increased its cyber security capability so that the Chief Executive and the Government Chief Digital Officer and the Government Chief Information Security Officer can be assured on an ongoing basis that Ministry websites are secure and fit-for-purpose. The Ministry has also implemented two-factor authentication for Ministry staff accessing internal systems remotely.

In future the Ministry will ensure risk and privacy assessments are carried out on all new external facing websites and that penetration testing is undertaken on any external or internal facing website that contains private information. Appropriate security testing will be undertaken for all other websites and web services as required by risk assessments.

The Ministry will also continue to adopt common ICT services where appropriate, noting the fit-for-purpose nature of many of these systems. The Ministry has several All-of-Government (AOG) common capability infrastructure systems already in use and its future digital strategy is to procure and use AOG web technologies wherever appropriate.