Summary Report

08 March 2022

Teaching Council adopts recommendations after reviews of privacy breach

Introduction

The Teaching Council of Aotearoa New Zealand is strengthening its internal policies and procedures after accepting recommendations from an external review into a privacy breach that occurred in December 2021.

The breach occurred as a result of human error rather than an external cyber incident. A staff member mistake led to a spreadsheet of information containing details of general enquiries and correspondence appearing on an online technology forum. The staff member copied an extract into a spreadsheet with the intention of seeking peer technical input to resolve a technical challenge they had been unable to resolve themselves relating to a particular piece of software used by the Council. The person receiving the information placed it on an online forum to seek advice.

The staff member had intended to delete all identifiable data from the spreadsheet. However, in error they omitted to delete a small number of columns of the large spreadsheet some of which contained information about identifiable individuals.

Once alerted to the matter, the Council contacted the Office of the Privacy Commissioner and all listed people.

In addition to an internal incident review, an independent review by professional director Jenn Bestwick was commissioned. The findings of the internal incident report and management discussions were shared with the external reviewer and factored into the external reviewer's report.

The investigation found the circumstances breached existing Teaching Council privacy, technology, information, and employee induction policies.

Recommendations include strengthening employee induction processes, establishing protocols for employees seeking external specialist support, and ensuring all policies and procedures remain current and are reviewed regularly.

Chief Executive Lesley Hoskin said, "The Teaching Council accept the findings and we are committed to implementing all recommendations. We are accountable for ensuring similar mistakes do not happen again and commissioned the investigation to understand where we need to improve our systems.

"While the external investigation found that in general the Teaching Council responded well to the breach, quickly moving to have the spreadsheet removed from the public site, advising the Office of the Privacy Commissioner, and communicating appropriately to those individuals deemed to be affected parties, we are disappointed that it happened in the first place.

"We are focussed on delivering on the recommendations to provide confidence to our members and to ensure ongoing accountability. We will confirm when all the recommendations have been implemented.

"We will take the learnings from this incident and do all we can to ensure this type of mistake does not happen again. It is clear that privacy protection must be a priority to ensure teachers can have confidence in our systems and processes.

"We have contacted the 55 individuals deemed to have been affected by the breach and an additional 141 named parties, and we apologise again for the mistake," said Ms Hoskin.

A full copy of the external review report is available here.

Terms of reference

The Terms of Reference for the external review focused on five distinct areas:

A. Providing information and advice to the Chair of the Governing Council
B. Providing information and advice to the Governing Council
C. Advising those deemed affected by the privacy breach
D. Advising the Minister of Education
E. Issuing of a public statement.

The reviews' findings

The investigation found the employee breached existing Teaching Council privacy, technology, information, and employee induction policies.

It also found the Teaching Council failed to ensure the employee completed their induction in a timely manner, which may have contributed to a lack of knowledge of understanding of relevant policies and procedures. The external reviewer noted that this relates to the "one deep" nature of the person's role. The employee was employed amongst other things, specifically to work on a particular piece of software and to bring data extraction and analytics skills using common tools and query languages in-house (the role previously having been outsource by contractors). The external reviewer believed the Council failed to consider how the employee was intended to obtain technical support and as such did not communicate its expectations to the employee in this regard. This may have contributed to the employee's lack of knowledge or understanding of the Council's policies and procedures relevant to the incident.

Once alerted to the breach, the Teaching Council initially assessed 44 people met the criteria to be deemed affected parties and subsequently contacted them. After further review by an independent privacy expert, the Council determined that an additional 11 people should be deemed affected parties, meaning there was a total of 55 affected people in total. The privacy of a further 141 individuals included in the file was deemed not to have been breached due to the nature of the personal information involved.

The external investigation found the Teaching Council's assessment of those affected by the breach was reasonable and there is no evidence of any attempt to minimise or downplay the number of affected parties.

It finds the assessment was undertaken with urgency driven by a desire to notify affected parties directly ahead of any media coverage. This may have contributed to taking a slightly narrower interpretation of affected parties than might otherwise have been the case.

The external review found that, on balance, contacting the wider group of all individuals involved in the breach would have been unlikely to cause harm and would have better supported the maintenance of trust and confidence in the Teaching Council. The reviewer notes this may not be strictly consistent with privacy practice, but in applying a wider strategic lens believes it is justifiable in this particular instance.

All individuals have since been contacted by the Teaching Council.

The external review also found that engaging expert communications advice would have been likely to improve the efficacy of the response and enable the Council to better manage their engagement with the media.

The Terms of Reference required the external investigation to consider whether the Teaching Council Chief Executive acted reasonably and in good faith during this process.

The external investigation found the Chief Executive acted reasonably and in good faith in advising those deemed affected by the privacy breach, providing information and advice to the Chair and Governing Council of the Teaching Council, and in issuing public statements.

The external reviewer also noted there is nothing to suggest that the Chief Executive acted other than in good faith in relation to all parties. It also noted the Chief Executive's directive to the Incident Response Team was for full disclosure of the information disclosed where individuals were deemed to have been affected.

In advising the Minister of Education, the Chief Executive's initial phone briefing to the Minister of Education's office on the morning of 10th December could have been more fulsome. The Chief Executive advised the Minister's office of the assessed number of affected parties, that some of the information was considered sensitive and advised that the Council was notifying those parties directly. The full extent and detail of the sensitive nature was not communicated to the Minister's office at this time due to the Chief Executive's caution that this may have represented a further breach of privacy.

At the point at which the Chief Executive initially notified the Minister's office in accordance with the no surprises convention, the Incident Response Team had identified the number of affected parties which was, and remains, a relatively small number and the nature of the information disclosed was known. The Chief Executive contacted the Minister's office consistent with the "no surprises" convention and updated the office on a regular basis over the next fortnight.

The external reviewer noted the Chief Executive indicated she was wrestling with whether a more detailed disclosure would have represented a further privacy breach, and accordingly she took a conservative approach in indicating that the breach contained sensitive information, but not the full detail of that information. Given this, the external review found the Chief Executive acted in good faith in providing information to the Minister, but by not fully disclosing the nature and scope of the disclosure, due to her concern regarding a further privacy breach, she only partly met the reasonableness requirement.

Separate to the issue of whether the Chief Executive acted reasonably and in good faith in providing information and advice to the Governing Council of the Teaching Council, the external review considers one area of the response that was not well managed was the interface between the Governing Body and the Executive.

The external reviewer noted there was not any formal written evidence that the Governing Body made any decisions in relation to the incident, made formal delegations to the incident team, and that it should have appointed a subset of members to work with the Incident Response Team both to bring governance input and decision making, and to provide a channel of communication between the executive and the wider Governing Body.

The external investigation found the Teaching Council has a range of frameworks, policies procedures relating to information security and has significantly matured in this area in recent years.

It also considers the Teaching Council to have strong practices in reinforcing these to all staff and providing illustrations of the expected behaviours, such as by including information security and privacy "stand-ups" at quarterly staff meetings.

Recommendations

Based on its findings, the external investigation provided the following six key recommendations:

1. Strengthening on-boarding and induction processes to ensure they are more closely managed and consistently applied so all new employees understand the organisational policies and procedures and their own individual responsibilities.
2. Establishing operating protocols for "one-deep" specialist roles, recognising the need for employees in those roles to seek external peer support and advice when there is no other specialist expertise within the organisation, and ensuring they are supported to fulfil their role safely
3. Continue to build the organisation's information security and privacy cultures, raising awareness of individual responsibilities in relation to both information security and privacy
4. Ensure all policies and procedures remain current and are reviewed within the documented review windows.
5. Continue to implement the recommendations of the recent Protective Security Requirements Information Security Assessment
6. Review its Incident Response Plan and protocols to include the establishment of a Governing Council incident response team, the development of protocols for communications, and a channel of communication between the executive and the wider Governing Body.

Implementation of recommendations

The Council has already begun to implement the recommendations. To date, it has:

- Ensured all staff are aware of the key policies and procedures relating to information security and privacy
- Strengthened on-boarding, induction processes and support for specialist staff working in one-deep roles
- Expedited the review of relevant policies and procedures to ensure they are current.

The remaining recommendations, such as establishing a Governing Council incident response team and communication protocols, implementing the recommendations of the recent Protective Security Requirements Information Security assessment, and strengthening the Council's internal information security culture, will be implemented by 30 June 2022.