Independent Review of Privacy Breach

Teaching Council of New Zealand

February 2022

1. Acknowledgement

New Zealand law clearly establishes a framework and sets an expectation that an individual's privacy including their personal information should be protected in accordance with internationally recognised privacy obligations and standards relating to the privacy of personal information. New Zealanders have a right to be able to expect their information is managed in accordance with that framework.

The Review wishes to acknowledge the individuals impacted by the disclosure of their personal information by the Teaching Council of New Zealand.

The Review also wishes to acknowledge the interviewees for their openness, honesty and co-operation with the Review.

Jenn Bestwick
Reviewer

Table of Contents

Executive Summary

4. At approximately 11.10am the Teaching Council of New Zealand (the Council) was alerted to a potential Privacy Breach via email from a TVNZ Legal Advisor to the Council's Enquiries email address. TVNZ advised the information had been discovered by one of their reporters investigating an unrelated matter.
5. The information disclosed included information collated by the Council for the purposes of monitoring general enquiries and correspondence and contained sensitive information about a number of individuals.
6. The Council immediately set up an incident response team and worked to contain and respond to the incident over the coming days.
7. The breach occurred as a result of a series of action triggered by a Council employee who copied a extract from the Council's JIRA Platform into a spreadsheet with the intention of seeking peer technical input to resolve a technical issue.
8. The employee intended to delete all identifiable data from the spreadsheet however in error they omitted to delete a number of columns of the large spreadsheet some of which contained information about identifiable individuals.
9. The employee shared the information with a former colleague and technical peer most likely on the 16th October 2021. Without the knowledge of the employee, after trying to resolve the issue themself, the former colleague posted the information to a technical forum on 20th October 2021 to seek input from other technical specialists into resolving the issue.
10. It was on this forum that the TVNZ reporter discovered the data.
11. Approximately one week after the incident the governing body of the Teaching Council commissioned an independent review of the incident. The findings of the review are included below.

Finding and Recommendations

The Cause of the privacy breach

12. The Review finds that:
    a. The circumstances and facts of the incident constitute a breach of the following Council policies and procedures:
        i. Statements 8, 9, 11, 12 of the Information and Records Management Policy
        ii. Statement 10 of the Information Release Policy
        iii. Statement 5 of the ICT Acceptable Use Policy
        iv. Privacy Commitment 2 of the Privacy Policy
        v. Procedures 12 & 14 of the Use of Technology Procedures
        vi. Procedures 56, 62,67 and 68 of the Recruitment and Induction Procedures
    b. The Council failed to consider how the employee whose actions precipitated the breach was intended to obtain technical support and did not communicate its expectations to the employee in this regard.

c. The failure of the Council to ensure the employee completed their induction may have contributed to the employee's lack of knowledge or understanding of the Council's policies and procedures relevant to the incident.

The Adequacy of the Response

13. The review finds that in general the Council responded well and that the Incident Response Team operated in a manner consistent with commonly accepted incident response practices.
14. The review considers the drive to communicate with parties deemed to have met the criteria for potential for serious harm under s113 of the Privacy Act 2020 to be laudable and that the tone, content, timeliness and transparency of the communication was appropriate.
15. The review finds that the Incident Response Team's assessment of the individuals who met the criteria of serious harm was reasonable given the subjective nature of the assessment criteria and that there is no evidence of any attempt to minimise or underestimate the number of affected parties.
16. However the reviewer does consider that the rushed nature of the assessment possibly contributed to taking a slightly narrower interpretation of affected parties than might otherwise have been the case had they taken slightly longer to consider the information disclosed.
17. On balance the review is of the opinion that contacting the wider group of named individuals would have been unlikely to cause harm and was likely to have supported the maintenance of trust and confidence in the Council by the profession, particularly given the information held by the media outlet that discovered the information.
18. The review finds that engaging expert communications advice would have been likely to improve the efficacy of the response and have enabled the Council to better manage their engagement with the media.

Whether the Chief Executive acted reasonably and in good faith

19. The review finds that the CEO acted reasonably and in good faith in advising those deemed affected by the privacy breach.
20. The review finds that the CEO acted reasonably and in good faith in providing information and advice to the Chair of the Governing Council.
21. The review finds that the CEO acted reasonably and in good faith in providing information and advice to the Governing Council.
22. The review finds that the CEO acted in good faith in relation to providing information to the Minister of Education. In not fully disclosing the nature and scope of the disclosure initially due to her concern regarding a further privacy breach the review finds that she acted reasonably however the review considers it would have been preferable for the Minister to have received a more fulsome briefing and that had further advice been taken/received by the CEO that this may have occurred.
23. The review finds that the CEO acted reasonably and in good faith in issuing public statements.

Appropriateness and effectiveness of Information Security

24. While no system is completely immune to human error there are areas in which the Council could strengthen its information security as highlighted by this incident, and recommends the following:
    a. Strengthening on-boarding and induction processes ensuring they are more closely managed and consistently applied to ensure all new employees understand the organisational policies and procedures and their individual responsibilities and accountabilities.
    b. Establishing operating protocols for "one-deep" roles within the organisation recognising the need for employees in those roles to seek external peer support and advice and ensuring they are supported to fulfil their role safely.
    c. Continuing to build the organisation information security and privacy cultures and raising awareness of individual responsibilities in relation to both information security and privacy.
    d. Ensuring all policies and procedures remain current and are reviewed within the documented review windows.
    e. Continuing to implement the recommendations of the recent Protective Security Requirements Information Security Assessment.

Any other relevant matters necessary to provide a complete report

25. That the Council reviews it's Incident Response Plan and protocols to include the establishment of:
    a. A Governing Council incident response team; and
    b. Protocols for communication to the Governing Council in such situations.

Introduction

27. At approximately 11.10am on the 9th December 2021 the Teaching Council of New Zealand (the Council) was alerted to a potential Privacy Breach via email from a TVNZ Legal Advisor to the Council's Enquiries email address. TVNZ advised the information had been discovered by one of their reporters investigating an unrelated matter.
28. The information purported to have been disclosed included information collated by the Council for the purposes of monitoring general enquiries and correspondence and contained some sensitive information.
29. Post responding to the incident the Council has conducted its own internal review of the Incident.
30. On 21st December 2021 I was appointed by the Council's governing board to undertake an Independent Review of the Privacy Breach to consider the following:
    a. the circumstances surrounding and cause of the incident;
    b. the adequacy and appropriateness of the incident response;
    c. the appropriateness of the Council's information security controls including its policies, processes, governance and practice; and
    d. whether the Chief Executive acted reasonably and in good faith in relation to the incident and in advising relevant parties
31. The full Terms of Reference for the Review are contained in Appendix A of this report.

The Incident

What occurred – the circumstances surround in the incident and the Incident Response

33. The following timeline outlines the pertinent actions that occurred in relation to the incident.

9th December 2021

34. At approximately 11.10am on the 9th December 2021 the Teaching Council of New Zealand (the Council) was advised of a potential Privacy Breach via email from a TVNZ Legal Advisor. The email was sent to the Council's Enquiries email address.
35. The ICT Manager initially found the email forwarded it to the Council's Government Relations and Information Manager (GRIM) who also holds the Privacy Officer role for the Council for review. The email contained an embedded link to the document containing personal information of a number of correspondents with the Council.
36. The GRIM recognised the information as an extract from the Council's JIRA board used to track general correspondence, complaints and information requests.
37. At 11.35 the GRIM escalated the issue to Deputy Chief Executive – Operational Services (DCE – OS) and Chief Financial Officer (CFO).
38. The Chief Executive Officer (CEO) was advised at 11.40am and stood up an incident response team comprising of the CEO, ICT Manager, GRIM, Communications Advisor and CFO. The DCE - OS was appointed the Incident Manager.
39. The GRIM advised the Incident Response Team that the incident constituted a notifiable breach under Part 6, of the Privacy Act 2020 and was instructed to proceed with notification the Office of the Privacy Commissioner (OPC) in accordance with s114 of the Act. The notification form was completed and submitted to the OPC at 12.23pm.
40. At 12.55pm the CEO contacted the Council Governing Body Chair (the Chair) to advise of the incident and left a message asking the Chair to call her urgently. The Chair returned the CEO's call and was briefed on the incident. The Chair notified the Governing Body by email at approximately 3pm.
41. In the meantime the Incident Response Team proceeded to investigate the possible sources of information initially considering the information had been accessed via some sort of cyber event or other unauthorised access.
42. The location of the information was identified as being a subscription only technical forum thread operated by Enterprise DNA and the information was confirmed as an extract of the spreadsheet information contained in the Council's JIRA Board.
43. In the course of working to identify how the information had been accessed a Council employee, [redacted] (the employee), recognised the data and immediately disclosed that in October 2021 they had sought assistance

from a former technical colleague in October regarding a piece of software used by the Council to provide business analytics, Power BI and had provided what they had believed to be anonymised data to the former colleague via a USB stick to enable them to provide technical assistance.

44. The employee contacted the former colleague who confirmed they had posted the information on the Enterprise DNA technical forum on 20th October 2021 in an attempt to resolve the technical issue the employee had been working on.
45. At 1.20pm the Council made contact with Enterprise DNA and requested them to remove the technical thread on its Forum. Various challenges locating the thread meant the information was not taken down from the website until 9.53pm on the 9th December. Enterprise DNA confirmed removal of the file from their asset library at 10.46pm and at 05.15am on the 10th December confirmed no cache version of the file remained in WebArchive or Google caches.
46. The Council advised the National Cyber Security Centre of the incident and received confirmation the appropriate government agency to liaise with was the OPC.
47. In parallel to the activity to contain the breach, the Incident Response Team directed the CFO and the employee to conduct an initial line by line assessment of the potential serious harm to affected individual (under s 113 of the Privacy Act 2020). This initial assessment identified approximately 50 individuals.
48. Independently the initial assessment of affected individuals was reviewed by the Council's Privacy Officer (the GRIM) applying the same s113 criteria.
49. Once that review was concluded the CEO and DCE - OPS reviewed the entire spreadsheet including the list of individuals identified by both prior assessments and seeking further expert input from the Privacy Officer as required before finalising the assessment. At the conclusion of these reviews the number of rows of the spreadsheet considered contain information relating to individuals that met the criteria of serious harm under s113 of the Privacy Act 2020 was deemed to be 43.
50. Draft communications to affected parties and other stakeholders were drafted.

10th December 2021

51. The Incident Response Team met to review the draft communications material and at 10.36am and 10.40am respectively the CEO contacted the Chair and Board Communications Committee Chair asking them to review the draft communications material.
52. The CEO notified the Minister of Education's office and the Secretary of Education of the incident.
53. Early in the afternoon of the 10th the Council contacted each of the 43 individuals and one organisation assessed as having met the criteria for potential serious harm under s113 of the Privacy Act 2020 and advised them of the breach and the information about them that had been disclosed.
54. In the early afternoon the OPC contacted the Council to advise that TVNZ had advised they were aware of file summary information remaining accessible in Google search results and suggested the Council may wish to contact Netsafe to assist in ensuring there were no further references to the information available.
55. The Council contacted Enterprise DNA and advised on how to remove the Google search cache results.

11th December 2021

56. The Council sought further confirmation from Enterprise DNA that the Google search cache results had been removed.
57. The ICT Manager contacted Google to have the broken link to the file removed from the cached search results.

12th December 2021

58. The cache was confirmed as removed by Enterprise DNA at 5.55am and later verified by the ICT Manager on the 12th December.
59. The Council's legal advisors wrote to TVNZ requesting they delete all copies of the information and not retain or use the information in any way. The review understands TVNZ has refused to confirm they have deleted the information.

13th December

60. The Council received written confirmation from the former colleague of the employee who posted the spreadsheet on the technical forum that they:
    a. no longer were in possession of the original dataset or any copies (regardless of format).
    b. did not have any other Council data provided by the employee.
    c. did not have any file on any shared platform for which they had access, such as Microsoft OneDrive etc.
    d. had not shared the files with any other third-parties other then EnterpriseDNA and that also have been removed.
61. TVNZ invite the CEO to be interviewed regarding the privacy breach. The CEO consulted with the Chair and Board Communications Committee Chair who agreed that the interview should proceed.

15th December

62. The CEO was interviewed on camera by TVNZ.

16th December

63. The Council advised approximately 157,000 teachers of the privacy breach and advised that if they had not been previously contacted by the Council they were not impacted by the breach.
64. TVNZ ran the story airing the interview with the CEO.

17th December

65. The Minister of Education suggested the Council undertake an Independent Review.
66. At the Council's Governing Body meeting the CEO briefed the Governing Body regarding the incident at its meeting and the Governing Body agreed to commission an Independent Review .

22 December

67. The Council announced it would undertake an Independent Review.
68. TVNZ ran second story suggesting the Council has understated the extent of the privacy breach.

How did it occur – Controls and Policies review

69. The review has considered the control environment, policies and procedures operative and relevant to the incident at the time at the Council.
70. In recent years the Council has introduced a suite of information security, information management and privacy policies and procedures which are appropriately owned by the Governing Body and managed through the Governing Body's Risk, Audit and Finance Committee. These are Governing Body policies and are reviewed on a regular cycle (either 2 or 3 yearly dependent on the policy) with regular monitoring of the Council's performance featuring on the Governing Body's dashboard reporting.
71. In addition despite not being part of the Public Sector, the Council has chosen to adopt the New Zealand Protective Security Requirements and has undertaken two audits against the Protective Security Requirements, the most recent being November 2021. The most recent report indicates the Council has made significant progress towards improvement of its information security control environment with a number of areas identified for further improvement. In the reviewer's opinion the most recent audit indicates the Council is reaching an acceptable level of maturity for an organisation of its size and role. There are always ways in which an organisation's protective security can be improved and the Council's response to the recent audit indicates it is seeking to further improve is maturity in this area.
72. Over the last two years the Governing Body, through its Risk, Assurance and Finance Committee has either reviewed or developed a range of policies and procedures relating to risk and to information security and privacy risk in particular. The suite of organisational policies relevant to the incident are documented in the Councils' ICT Security Management Framework (adopted by the Governing Body in November 2019) and include the:
    a. IT Acceptable Use Policy – approved by the Governing Body in November 2019
    b. Information and Records Management Policy – approved by the Governing Body in August 2021
    c. Information Release Policy – approved by the Governing Body in August 2021
    d. Privacy Policy – approved by the Governing Body in November 2020
    e. Use of Technology Procedures – approved by the Governing Body in Nov 2019

73. Also relevant to the incident is the Council's Recruitment and Induction Procedures adopted by the Governing Body in June 2018 and which was due for review in June 2021.
74. The Council's Cyber risk register identifies the risk that a Council employee either deliberately or accidentally accesses personal information or makes that access available to others (Risk PR16) as one of its top risks. It rates the risk as possible and the impact as significant indicating that the organisation was alert to the risk. At its November meeting the RAF Risk Register identified the residual risk (after mitigations) as High.

Review of Policy Framework and Procedures

75. The ICT Security Management Framework provides the umbrella framework for the security of information at the Council and utilises the New Zealand Information Security Manual and New Zealand Protective Security Requirements as the basis for its design. Accordingly the Framework addresses the full range of PSR principles and requirements (excluding the requirements related to classified information).
76. Security governance is clearly articulated with roles and responsibilities documented and Chief Information Security Officer (CISO) and Chief Security Officer (CSO) roles appointed by the Council. One minor point to note is that the review understands responsibility for the CISO role changed in 2021 from the DCE - OPS to the ICT Manager. The framework has not reviewed and updated with this change in responsibility.
77. As previously noted the framework outlines the suite of policies and procedures providing the security architecture for the organisation. The following paragraphs examine the areas relevant to the incident.

Information & Records Management Policy

78. The purpose of this policy is stated as being "to outline the high-level data and information policy statements for the Council to ensure that data and information are well managed to support the Council as the professional body for the teaching profession". It contains a number of policy statements, of which the relevant statement to this incident is under the heading of "Protect and Respect".
79. The policy statements relevant to the incident are as follows:
    a. "Statement 8 - The Council will protect and respect the data and information which we create or are entrusted with.
    b. Statement 9 - The Council recognises that the teacher's data and information which we collect and care for is a national taonga. To retain the trust and confidence of the teaching profession, we will treat the data and information with the utmost respect..
    c. Statement 11 - All employees will attend privacy and information management training.

d. Statement 12 - The Council will ensure personal, in-confidence and sensitive data and information are protected. This includes data and information about teachers, employees, commercially sensitive and security classified data and information."

Information Release Policy

80. The purpose of this policy is stated as being "to ensure the Council releases information in an appropriate way which adheres to the Privacy Act 2020 and the Official Information Act 1982".
81. The Policy Statements relevant to the incident are as follows:
    a. "Statement 10 - Personal information must not be released except as permitted by law."

ICT Acceptable Use Policy

82. The purpose of this policy is stated as being "to specify the Council's requirements for staff and contractors when using information and communications technology".
83. The Policy Statements relevant to the incident are as follows:
    a. "Statement 5 – Personal devices are not to be used for Council business, to be connected to Council computer equipment, or to be used to access or store Council data and information
    b. Statement 6 – Staff and contractors must not compromise the safety of Council systems and processes"

Privacy Policy

84. The purpose of this policy is stated as being "to explain how the Council collects, uses, stores and shares personal information it collects".
85. The Privacy Commitment relevant to the incident is as follows:
    a. "Commitment 2 – We will only use and share personal information where necessary to carry out the functions for which we collected it, or if required by law or in accordance with legislation"

Use of Technology Procedures

86. The purpose of these procedures are stated as "to set out the procedures that are to be followed by staff and contractors when using information and communications technology at the Council. These procedures contribute to the safety and security of information and communications technology at the Council and the data held on those systems".
87. The procedures relevant to the incident is as follows:
    a. "Procedure 12 – Using personal devices at the Council.
        i. Personal devices are not permitted to be used for Council business.
        ii. Personal devices are not to be connected into Council computers or mobile devices, e.g. USB sticks, headphones, charging cables and blue tooth devices
    b. Procedure 14 – Removable devices

i. Staff and contractors must not use removable devices for the transfer of Council data or information".

Recruitment and Induction Procedure

88. The purpose of this policy is stated as being "to ensure the standardisation of recruitment processes to ensure the best possible applicant is appointed and to set out the processes for inducting employees new to roles so they are educated and prepared for roles and can quickly be efficient and effective".
89. The procedures relevant to the incident are under the Induction heading as follows:
    a. "Procedure 56 – The reporting manager will be responsible for organising the orientation and induction programme by either directly carrying out or arranging to have parts of the programme carried out by other employees.
    b. Procedure 62 – As a result of the orientation and induction programme it is expected all new employees will:
        i. Understand the professional and behavioural standards required of all Council employees (including the Code of Conduct)
        ii. Understand the Council's policies particularly those concerning information management, security and protection from Privacy Act breaches, basic workplace procedures
    c. Procedure 67 – The Hiring/Reporting Manager shall organise orientation and induction programme to be carried out by manager and other employees
    d. Procedure 68 – HR shall be responsible for keeping track of induction completion".

Findings and Recommendations

The Cause of the Privacy Breach

91. The review considers the source of the breach to be well understood. The breach occurred as a result of a series of action triggered by a Council employee employed as [redacted] copied a extract from the Council's JIRA Platform 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.
92. The employee intended to delete all identifiable data from the spreadsheet as the only fields required to resolve the issue related to a unique identifier, and two date fields. However in error they omitted to delete a small number of columns of the large spreadsheet some of which contained information about identifiable individuals.
93. The employee copied that spreadsheet onto a USB stick and shared the information with a former colleague and technical peer most likely on the 16th October 2021. Without the knowledge of the employee, after trying to resolve the issue themself, the former colleague posted the information to a subscription technical forum on 20th October 2021 to seek input from other technical specialists to resolving the issue.
94. For clarity, there is absolutely nothing to suggest that either the employee or their technical colleague's actions were intentionally or maliciously intended to cause the privacy breach.

Contributing Factors

95. There are a number of wider factors the review considers relevant to the cause of the incident:
    a. The employee had only recently joined the Council on 13th September.
    b. Due to the view that the priority was for the employee to maximise the hand-over opportunity to sit alongside the out-going contractor who had previous performed the role at the Council, the employee had only partially completed their induction into Council procedures at the time of the incident.
    c. The employee had received the ICT Acceptable Use Policy, ICT Use of Technology Procedures and Standards of Integrity and Conduct information as part of the offer of employment and confirmed in writing that they had read and understood, however they did not complete their Privacy Induction briefing until 21 December 2021, the ICT Induction Briefing until 17 December 2021 or the Online Privacy Module until 21 December 2021.
    d. The [redacted] expertise required by the employee role is a "one deep" role in the organisation and as such there is no

other specific technical expertise in the Council able to assist the employee in their work.

e. The employee reported into the [redacted]. While the [redacted] was able to provide general management advice and guidance they were not in a position to provide any technical advice or guidance. The employee had started to build connection with the ICT team at the Council, however there was no formal mechanism in place for this to occur and the ICT team had limited experience working with the software in question.

96. The review considers there are two material issues outlined above that may have contributed to the incident. Firstly the fact that the employee had not been fully inducted into the Council makes it difficult to assess whether the employee had full knowledge of the Council's policies and procedures at the time of the incident. By signing the employment contract and confirming that they had read and understood the attached policies it should be assumed that they understood their responsibilities in relation to :
    a. Statements 5 & 6 of the ICT Acceptable Use Policy
    b. Procedure 12 & 14 of the Use of Technology Procedures.
97. However it is less clear that the employees obligations under the following policies had been communicated to the employee ahead of the incident:
    a. Information and Record Management Policy;
    b. Information Release Policy; or
    c. Privacy Policy.
98. It is also apparent that the Council had not complied with its own policy in relation to the induction of the employee both in relation to the responsibilities of the manager to arrange the induction and those of Human Resources to keep track of the completion of the induction process.
99. The second material issue relates to the "one deep" nature of the 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 consequence of this is that there was limited capability inside the organisation to provide technical support or mentoring and the employee's only way to obtain that technical support is by going outside the organisation.
100. The Council doesn't not appear to have considered this or provided guidance or "guard-rails" to ensure the employee was operating in a safe manner and in accordance with the Council's policies.

Findings

101. The incident constitutes a breach of the following Council policies and procedures:
    a. Statements 8, 9, 11, 12 of the Information and Records Management Policy
    b. Statement 10 of the Information Release Policy
    c. Statement 5 of the ICT Acceptable Use Policy
    d. Privacy Commitment 2 of the Privacy Policy
    e. Procedures 12 & 14 of the Use of Technology Procedures
    f. Procedures 56, 62,67 and 68 of the Recruitment and Induction Procedures

102. 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.
103. The failure of the Council to ensure the employee completed their induction may have contributed to the employees lack of knowledge or understanding of the Council's policies and procedures relevant to the incident.

Adequacy of the Response

104. The Council's response upon being advised of the potential privacy breach was generally well executed. The speed with which an Incident Response Team was stood up and allocated with tasks to support the response was rapid and targeted the key areas to contain the incident. The Incident Response Team adopted a standardised four stage response framework.
105. The Incident Response Team quickly identified the incident met the criteria of a notifiable event under the Privacy Act 2020 and completed the notification form on the OPC's website.
106. The Incident Response Team's process for identifying affected parties (consistent with the Privacy Act 2020) was considered with at least three reviews of the information released including one by the Privacy Officer. The initial review considered all lines in the spreadsheet and identified a number of parties who potentially meet the criteria of serious harm. This was subsequently independently reviewed by the GRIM. Both the subset of individuals identified in these two reviews and the full spreadsheet were then reviewed by the CEO and DCE - OPS and a determination made that 43 individuals were identified as having met the criteria for potential serious harm under s113 Privacy Act 2020.
107. One of the accusations the Council has faced following the breach is that it has "minimised" or "under-estimated" the number of people considered to be affected parties. The Council has had its assessment of affected parties peer reviewed by an independent privacy expert. That peer review has indicated that the Council may have failed to include 11 further people in the assessment of affected parties. The review understands the Council is communicating with those additional individuals and that a separate letter has been sent to all individuals identified but not deemed as having met the s113 criteria for the purposes of clarification.
108. The criteria for determining whether an individual is likely to suffer serious harm is specified in s.113 of the Privacy Act 2020 and states that the agency must consider:
    a. Any action taken by the agency to reduce the risk of harm following the breach:
    b. Whether the personal information is sensitive in nature:
    c. The nature of the harm that may be caused to affected individuals;
    d. The person or body that has obtained or may obtain personal information as a result of the breach (if known);
    e. Whether the personal information is protected by a security measure;
    f. Any other relevant matters.

109. As can be seen the test is subjective and requires the organisation applying the criteria to exercise a number of judgements relating to the unique circumstances of the incident. The Council's assessment was undertaken with urgency driven by a desire to be able to notify the affected parties urgently and ahead of any public commentary in the media. Had the Council taken slightly longer to undertake the assessment they may have chosen to include the relatively small number of additional individuals identified in the peer review in their assessment. However there is nothing to suggest the Incident Response Team acted in other than in good faith in their conduct of the assessment.
110. The content of communication to the affected parties identified by the Council was transparent, sincere and timely and included full disclosure of all the information relating to the affected party included in the breach. The Council anticipated and responded well to the queries and responses this communication generated and while for obvious reasons, some affected parties may have been dissatisfied with their engagement with the Council, the information considered by the review indicates the Council's follow-up communication with those individuals who contacted the Council was transparent, respectful and appropriate.
111. The Incident Response Team decided early to have fulsome communication with the parties deemed to have met the criteria for potential serious harm. With regard to the individuals who were included in the breach but whom were not assessed by the Incident Response Team to have met the threshold of serious harm, the rationale for not notifying was reportedly the risk of causing more harm than not notifying. Once again this represents a judgement call. Privacy experts interviewed by the review were divided on whether communicating with individuals not deemed to have met the criteria of serious harm would have been appropriate or not. The judgement appears to rest on whether you place more weight on:
    a. the risk of harm to the individual by notifying parties whose information is not judged as meeting the threshold of serious harm but who are included in the breach; or
    b. the wider issue of the importance of maintaining the trust and confidence of the profession in the Council.
112. On balance the review is of the opinion that contacting the wider group of individuals would have been unlikely to cause harm and was likely to have supported the maintenance of trust and confidence in the Council by the teaching profession, particularly given that the information was held by the media outlet that discovered the information.
113. One aspect of the response that could have been strengthened in the view of the reviewer is the involvement of expert communications advice in the Incident Response Team. Given the seriousness of the incident, having senior communications expertise involved from the outset would have most likely assisted the Council's stakeholder and media management and supported the Incident Response Team. This appears to have been quite a significant omission in the response and one which may have resulted in the Council receiving greater adverse stakeholder and media reaction.

Findings

114. The review finds that in general the Council responded well and that the Incident Response Team operated in a manner consistent with commonly accepted incident response practices.
115. The review considers the drive to communicate with parties deemed to have met the criteria for potential for serious harm to be laudable and that the tone, content, timeliness and transparency of the communication was appropriate.
116. The review finds that the Incident Response Team's assessment of the individuals who met the criteria of serious harm was reasonable given the subjective nature of the assessment and there is no evidence of any attempt to minimise or underestimate the number of affected parties.
117. However the reviewer does consider that the rushed nature of the assessment possibly contributed to taking a slightly narrower interpretation of affected parties than might otherwise have been the case had they taken slightly longer to consider the information disclosed.
118. On balance the review is of the opinion that contacting the wider group of named individuals would have been unlikely to cause harm and was likely to have supported the maintenance of trust and confidence in the Council by the profession, particularly given the information held by the media outlet that discovered the information. The reviewer acknowledges this may not be strictly consistent with privacy practice and as such be controversial amongst privacy experts but in applying a wider strategic lens believes it is justifiable in this particular instance.
119. The review finds that engaging expert communications advice would have been likely to improve the efficacy of the response and have enabled the Council to better manage their engagement with the media.

Whether the Chief Executive acted reasonably and in good faith

120. The Terms of Reference required the review to consider this matter under five distinct headings namely in:
    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 public statements
121. In New Zealand the obligation of "good faith" is largely applied in relation to Employment law which is less relevant to the considerations above. For the purposes of the review, the reviewer has applied the more ordinary meaning of the phrase namely acting with "honestly or sincerity of intention" (Concise Oxford Dictionary Twelfth Edition)
122. The definition of reasonableness is ordinarily "fair and sensible" with a secondary meaning of "as much as is appropriate or fair" (Concise Oxford Dictionary).

123. The test for reasonableness is objective and relative to the situation but tends to rely on whether an action can be justified as rational and proportionate. It does not require perfection but that the decision was reasonable:
    a. In the circumstances at the time is was made[1]
    b. That is was one that was open to be reached[2] and
    c. Is "within the limits of reason" [3]
124. In considering this matter is should be noted that the CEO was part of the Incident Response Team and so involved in all aspects of the response as well as fulfilling the CEO role.

Affected Parties

125. Firstly in relation to those deemed affected by the privacy breach, as outlined above, the evidence and documentation considered by the review points to the CEO's primary concern at all times during the response being those affected by the privacy breach and that this expectation was clearly communicated to the Incident Response Team. There is nothing to suggest that the CEO acted other than in good faith in relation to those individuals.
126. Also as outlined above, the key challenge to the CEO's actions is that she sought to minimise or under-estimate the extent of the privacy breach by misrepresenting the number of people potentially impacted.
127. As discussed above, the assessment of serious harm is a subjective judgement call based on the unique circumstances of the situation. There is no evidence to suggest that the CEO in any way tried to influence the assessment of impact by the Incident Response Team in terms of quantum of people affected or the seriousness of the potential impact. The only way the CEO may be seen to have been influencing the assessment was to seek an early assessment so that the Council could communicate with those deemed to be affected by the breach. While this may have impacted the fulsomeness of the assessment, it was not in breach of any good faith obligation or unreasonable given the desire to communicate with affected parties ahead of any media coverage of the breach.
128. Furthermore the CEO's directive to the Incident Response Team was for full disclosure of the information disclosed where individuals were deemed to have been affected.

The Chair of the Governing Council

129. Evidence and documentation reviewed by the reviewer indicates that regular and open communication was maintained between the CEO and the Chair at all times throughout the response. The Chair was involved in reviewing communications material, agreeing to the CEO being interviewed by the media and received regular updates from the CEO. The Chair has indicated that she is comfortable with the

[1] Taiaroa v Minister of Justice (Maori Option Case) 1995 1 NZLR 411 (CA) at 418 (DCE - Opske P)
[2] N R v District Court at Auckland (2014) NZHC 1919 at [8]
[3] New Zealand Fishing Industry Association v Minister of Agricultre and Fisheries (1988) 1 NZLR 544 (CA) (DCE - Opske P)

CEO's communication with her throughout the incident and was provided with information she required to stay abreast of the situation and inform the wider board.

130. There is no suggestion that communication was anything other than open and transparent and given the fast moving nature of the incident it appears to have been frequent and responsive. The reviewer does observe that there is little in the way of a formal record of the communication and it is not clear that the Chair and CEO established a clear understanding of expectations of communication or governance input into decision making.

The Governing Council

131. Communication with the wider Governing Body is less clear although the reviewer understands communication fell into two groups, the first being with the Governing Body's Communications Committee and second being with the full Governing Body. It's not clear to the review when, how or by whom the decision was made that the Communication's Committee should be the Council Committee to take the lead in working with the executive on the response (in addition to the Chair) but it appears that the Committee Chair and committee members were involved in reviewing communications material both to affected parties and the profession as a whole.
132. Documentation of the extent of consultation is light and it's unclear whether the Committee's involvement was for approval or consultation, however there is evidence that feedback from the Communication Committee was incorporated into communications material issued by the Council.
133. Communication with the wider Governing Body is not well documented. The Review understands that following the CEO's alerting the Chair to the incident that it was agreed the Chair would brief the Governing Body which she did on the afternoon of the 9th December via email. Following the initial notification there doesn't appear to have been any articulation from the Governing Body of their expectations of communication to the executive.
134. The next briefing of the full Governing Body was on the 17th December at the Governing Body's regular meeting. At this point the Governing Body was given a briefing of the response to that point including the basis of assessment of affected parties and had the opportunity to seek clarification or further information.
135. The review considers that more frequent communication with the full Governing Body during the initial period may have been appropriate but accepts there was no apparent articulation of this expectation by the Governing Body at the time.
136. There is nothing to suggest that the CEO withheld or refused to disclose any information to the Governing Body at its meeting of the 17th December.

Advising the Minister of Education

137. The CEO advised the Minister of Education's office by phone on the morning of 10th December. The CEO 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 CEO's caution that this may have represented a further breach of privacy.

138. When the media broke the story on the 16th December the nature and sensitivity of the information was in the public domain. At this point the Minister indicated he felt the Council should undertake an independent review.
139. In assessing the reasonableness of the communication, the context of the Council is a factor The Council is a body corporate established under the Education Act 1989 and continued under the Education Act 2020. The Minister of Education and the Associate Minister of Education are its responsible Ministers and hold a number of Ministerial powers in relation to the Council. Whilst not technically part of the public sector, the appointment of 6 of the Council's members by the Minister, obligations to consult with the Minister articulated in the Act and the requirement for the Council to report to the Minister and the House of Representatives via the select committee process indicate that the Council operates in a space where adherence with the public sector convention of "no surprises" would be an appropriate assumption.
140. At the point at which the CEO initially notified the Minister's office in accordance with the 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 CEO contacted the Minister's office consistent with the "no surprises" convention and updated the office on a regular basis over the next fortnight.
141. The key issue appear to be that the CEO did not fully disclosed early on the sensitive nature of the information disclosed to the extent normally anticipated under the "no surprises" convention. In making this decision the CEO has indicated she was wrestling with whether a more detailed disclosure would have represented a further privacy breach and accordingly took a conservative approach in indicating that the breach contained sensitive information but not the detail of that information.
142. Given the nature of the information was subsequently released by TVNZ there does appear to have been an under-communication of the nature of the sensitive information advised to the Minister's office and an underestimation the potential for public interest and hence Ministerial interest in a privacy breach of this nature. The consequence of this was that the Minister's office was not fully appraised of the issue when the media story ran the following week.
143. The review has considered whether this represents either a breach of good faith or unreasonable action by the CEO.
144. Firstly, the review does not consider there was any intention by the CEO not to act in good faith. The review considers at the point the CEO briefed the Minister's office, she did not have knowledge of the TVNZ coverage that was to follow. The review finds she did act in accordance with the "no surprises" convention in briefing the Minister's office regularly, however in the review's opinion the CEO could have included a more fulsome briefing while still maintaining the privacy of the individuals affected and that had she taken further advice from public sector agencies such as Te Kawa Mataaho, the Public Service Commission she may have received guidance on navigating both import considerations, namely not contributing to a further breach and fully discharging the "no surprises" obligations.
145. The review observes that the operation of the Council at arms-length from government means that the advice and assistance normally available to a public

sector agency in these situations were not automatically available and/or did not swing into action to support the Council in this instance.

146. It is clear that it would have been desirable for the Minister's office to have received a more fulsome briefing regarding the nature and scope of the incident and that this may have triggered additional support and advice for the Council from the public sector on its responsibilities in the public interest.
147. On the question of whether the CEO acted reasonably in this situation, the review considers it would have been reasonable for the CEO to have taken more steps to assure herself more fully that expectations under the "no surprises" convention were being discharged and that in this regard the reasonableness expectation was only partially met. The CEO was aware of the sensitive nature of some of the information disclosed and had she taken advice, would have potentially provided a more fulsome briefing earlier to the Minister's office while being able to assure herself that she was not contributing to a further breach of privacy. However, the review does consider the CEO's decision represented a decision that was open to be reached and as such was not unreasonable given the time at which it was reached.

Issuing Public Statements

148. In considering this the review has taken public statement to mean a statement made either to the public at large or to a large group where there can reasonably be no expectation that the statement would not be in the public domain. Accordingly there are three categories of statements the CEO made:
    a. Media releases issued by the Council.
    b. Media interview undertaken by the CEO.
    c. Emailed correspondence to the teaching profession.
149. Once again the core allegation is that the CEO attempted to minimise the breach by downplaying the seriousness and/or the number of affected parties. As articulated above, there is nothing to suggest the CEO acted in any way other than in good faith or reasonably in relation to the communications issued. The CEO was entitled to rely on the assessment of the number of affected parties identified by the Incident Response Team at the time. In the review's opinion the statements issued acknowledge the seriousness of the breach and do not attempt to minimise the sensitive nature of some of the information disclosed.

Findings

150. The review finds that the CEO acted reasonably and in good faith in advising those deemed affected by the privacy breach.
151. The review finds that the CEO acted reasonably and in good faith in providing information and advice to the Chair of the Governing Council.
152. The review finds that the CEO acted reasonably and in good faith in providing information and advice to the Governing Council.
153. The review finds that the CEO acted in good faith in relation to providing information to the Minister of Education. In not fully disclosing the nature and scope of the disclosure initially due to her concern regarding a further privacy breach the review finds that she acted reasonably however the review considers it would have been

preferable for the Minister to have received a more fulsome briefing and that had further advice been taken/received by the CEO that this may have occurred.

154. The review finds that the CEO acted reasonably and in good faith in issuing public statements.

Appropriateness and effectiveness of Information Security

155. As outlined earlier in this report the Council has a range of frameworks, policies and procedures in relation to information security. In recent years it has made significant gains in maturity in the area.
156. The review also considers the Council's practice is strong in some areas such as the inclusion of information security and privacy "stand-ups" at quarterly staff meetings reinforcing the importance of the same to all staff and providing illustrations of the "lived" behaviours sought.
157. As previously articulated the incident occurred through a combination of both human error and breaches of the operational policies and procedures.

Recommendations

158. While no system is completely immune to the above there are areas in which the Council could strengthen its information security as highlighted by this incident, and the review recommends the following:
    a. Strengthening on-boarding and induction processes ensuring they are more closely managed and consistently applied to ensure all new employees understand the organisational policies and procedures and their individual responsibilities and accountabilities.
    b. Establishing operating protocols for "one-deep" roles within the organisation recognising the need for employees in those roles to seek external peer support and advice and ensuring they are supported to fulfil their role safely.
    c. Continuing to build the organisation information security and privacy cultures to raise awareness of individual responsibilities in relation to both information security and privacy.
    d. Ensuring all policies and procedures remain current and are reviewed within the documented review windows.
    e. Continuing to implement the recommendations of the recent Protective Security Requirements Information Security Assessment.

Any other relevant matters necessary to provide a complete report

159. The review considers one area of the incident response that was not well managed was the interface between the Governing Body and the Executive. As previously stated the review does not consider the CEO acted other than in good faith and reasonably, however the review considers the interface could have been substantially improved had the Governing Body formalised its expectations of the executive and formally nominated a sub-group of members to act on the Governing Body's behalf in relation to the incident, complete with delegation of decision making authority.
160. One feature of the incident is that the Governing Body does not appear to have made any decisions in relation to the incident. While the Chair and Communications Committee Chair were involved in some decisions and were included in a number of communications from the executive, there does not appear to be any formal delegation by the Governing Body to those individuals in relation to the incident. As such it is unclear whether the Governing Body had expectations of greater involvement or not.
161. In situations such as the incident, it is common for a subset of the Governing Body to be appointed 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 extent to which this is integrated into the incident response is usually dependent on the nature of the incident and often reflective of the criticality of decision making and the seriousness of the incident. In the opinion of the review, the Council would have benefited from formally instigating a Governing Body Incident Team with a clear delegation from the Governing Body and clearly articulated expectations of communication to the full Governing Body.

Recommendation

162. That the Council reviews its Incident Response Plan and protocols to include the establishment of:
    a. a Governing Body incident response team; and
    b. Protocols for communication to the Governing Body.

Terms of Reference

Independent Review of the Teaching Council's Privacy Breach

Background

On 9 December 2021, TVNZ alerted the Teaching Council to a spreadsheet of information they had discovered in a New Zealand-based online technology forum. This spreadsheet contained details of general enquiries, correspondence and official information requests received by the Teaching Council.

On discovery the Council advised the Office of the Privacy Commissioner and convened an incident response team to address the breach.

Objective of the review

As the professional regulatory body for the teaching profession, the Council holds personal information relating to all teachers as well as sensitive and confidential information relating to those teachers engaged in disciplinary processes.

The security of personal and confidential information held by the Teaching Council is of fundamental significant to the operation of the Council and central to the Council's role in assuring public trust and confidence in teachers.

The objective of this review is to address concerns raised by this incident about the security of personal and confidential information held by Council, focusing on what happened, why it happened, the lessons learned, and the actions the Council needs to take to ensure that a similar incident will not happen again.

Scope of the review

The independent reviewer is to investigate, make findings on, and report to the Governing Council regarding:

- The circumstances surrounding this incident, including the adequacy of the response.
- The causes of this incident, including whether the Council adhered to its own internal policies relevant to personal and/or confidential information and to applicable good practice guidance for the public sector.
- The appropriateness and effectiveness of the information security that the Council had in place prior to the privacy breach. This will include an assessment of the relevant policies, processes, governance, capability and security culture and practice of the Council.
- Any implications for the Council's wider information security systems.
- Whether the Chief Executive acted reasonably and in good faith before taking the actions below in relation to the incident:
    - Providing information and advice to the Chair of the Governing Council
    - Providing information and advice to the Governing Council

- Advising those deemed affected by the privacy breach
- Advising the Minister of Education
- Issuing public statements

- Any other relevant matters necessary to provide a complete report on the above.

Out of scope

The review will not make any findings on whether there should be further steps taken to initiate disciplinary, civil or criminal proceedings in relation to any individual.

Appointment

The Governing Council appoints Ms Jenn Bestwick to undertake this enquiry.

Reporting

The reviewer is to report her findings to the Chair of the Governing Council in writing on or before 25 February 2022.

If Ms Bestwick identifies issues which may impact on the delivery of her report by 25 February 2022, she will notify the Chairperson as soon as possible with a view to finding an appropriate solution, which may include an extension of time.

Nicola Ngarewa 21 December 2021

Chairperson

Teaching Council of Aotearoa