Office of the Information Commissioner
Queensland

Follow-up of Report No. 1 for 2018-19

Awareness of privacy obligations

How three Queensland government agencies educate and train their employees about their privacy obligations

Report No. 3 to the Queensland Legislative Assembly for 2020-21

Copies of this report are available on our website at www.oic.qld.gov.au and further copies are available on request to:
Office of the Information Commissioner
Level 7, 133 Mary Street, Brisbane, Qld 4000
PO Box 10143, Adelaide Street, Brisbane, Qld 4000

Phone 07 3234 7373 or Freecall 1800 OIC QLD (1800 642 753)
Email administration@oic.qld.gov.au
Web www.oic.qld.gov.au

ISBN: 978-0-6489306-0-0

March 2021

The Honourable Curtis Pitt MP
Speaker of the Legislative Assembly
Parliament House
George Street
Brisbane QLD 4000

Dear Mr Speaker

I am pleased to present '*Follow-up of Report No. 1 for 2018-19 – Awareness of privacy obligations: How three Queensland government agencies educate and train their employees about their privacy obligations*'.

This report is prepared under section 135 of the *Information Privacy Act 2009* (Qld).

It outlines the progress the Public Trustee of Queensland, the Department of Seniors, Disability Services and Aboriginal and Torres Strait Islander Partnerships[1] and TAFE Queensland made in implementing the recommendations from the 2018 audit.

In accordance with subsection 193(5) of the *Information Privacy Act 2009* (Qld), I request that you arrange for the report to be tabled in the Legislative Assembly.

Yours sincerely

Rachael Rangihaeata
Information Commissioner

[1] Our original audit examined the former Department of Communities, Disability Services and Seniors. Under Public Service Departmental Arrangements Notice (No.4) 2020, this department was renamed the Department of Seniors, Disability Services and Aboriginal and Torres Strait Islander Partnerships.

Table of contents

Summary

This report is about the Public Trustee of Queensland (the Public Trustee), the Department of Seniors, Disability Services and Aboriginal and Torres Strait Islander Partnerships (the department)[2] and TAFE Queensland's progress implementing recommendations we made in our original audit.[3]

In 2018, we examined whether these agencies:

- identify education and training as a strategy for mitigating privacy and information security risks
- ensure their education and training material appropriately covers information privacy and information security
- educate and train their employees, at induction and as part of a periodical refresher program, on information privacy and information security.

At the time we concluded that:

> *The three audited agencies have recognised the value of educating and training their staff on information privacy and information security in mitigating privacy risks. However, the effectiveness of their training varies. This is because they have adopted different training content, set different requirements for completing the training and established different processes to make sure employees complete the training.*
>
> *All three agencies have one or more weak elements in how they educate and train their staff about their information privacy and security obligations. As a result, they do not mitigate their privacy risks as well as they could.*

We made one recommendation to the Public Trustee, four to the department and seven to TAFE Queensland. The agencies accepted all recommendations.

[2] Our original audit examined the former Department of Communities, Disability Services and Seniors. Under Public Service Departmental Arrangements Notice (No.4) 2020, this department was renamed the Department of Seniors, Disability Services and Aboriginal and Torres Strait Islander Partnerships.

[3] Office of the Information Commissioner (Queensland). 2019. *Awareness of Privacy Obligations: How three Queensland Government Agencies educate and train their employees about their privacy*. Available on our website www.oic.qld.gov.au

We also made four general recommendations to all government agencies[4]. These recommendations are not assessed in this follow-up report however they may form the basis of future audits.

Results and conclusions

Over the last two years the audited agencies have done significant work on educating their staff about their information privacy and security obligations. All 12 recommendations are fully implemented.

This improves the effectiveness of training and education as a mitigation strategy for information privacy and security risk.

All three agencies now mandate periodic refresher training and have set up systems and processes to monitor and report on training completion. Mandatory refresher training increases the likelihood of employees retaining their awareness of information privacy and information security risks.

The Public Trustee and TAFE Queensland have updated their information privacy and information security training to better reflect their policies and procedures. The department has also updated its privacy training to include practical scenarios.

Comprehensive, relevant and practical training content means employees are more aware of their obligations and the privacy and information security risks.

Agency comments

We provided a copy of this report to each agency for comment. We considered the agencies' views in reaching our conclusions and represented them to the extent relevant and warranted in this report. Agency comments are in the Appendix.

[4] 'All Queensland government agencies' means all government agencies subject to the Information Privacy Act 2009 (Qld) including Queensland government departments, statutory bodies, local governments, public universities, Hospitals and Health Services, and other public authorities.

1. Context

The community entrusts Queensland government agencies with their personal information. Agencies must handle personal information appropriately to maintain this trust. This includes protecting personal information against loss, unauthorised access and other misuse as set out in the *Information Privacy Act 2009*.

Agencies should train and educate their employees about information privacy and information security obligations. To be effective, training and education should be mandatory, regular and tailored to the context of each agency. Systems and processes should also ensure all employees complete mandatory training when due.

In 2018 we audited three agencies and examined how they educate and train employees about their obligations under the *Information Privacy Act 2009*. The original audit report was tabled in Parliament in February 2019.

In February 2020, the Crime and Corruption Commission (the CCC) tabled *Operation Impala Report on misuse of confidential information in the Queensland public sector*[5]. It stated that:

> *Developing and maintaining an effective information privacy culture relies on the adequacy of internal policies, education and awareness campaigns, and practical training. The use of de-identified case studies was found to be a very useful educative and training tool, as they provided real-life scenarios that helped staff interpret the intention of policies.*

The CCC made 18 recommendations, including[6] that agencies ensure the training:

- is developed and provided to all public sector employees prior to gaining access to any database that contains confidential information
- is developed and provided annually to all public sector employees who have access to confidential information
- reflects the respective ICT access and use policy, including references to the Criminal Code, the relevant public sector agency governing Act and the *Information Privacy Act*
- comprises a combination of online, face-to-face and video modules

[5] Available on www.ccc.qld.gov.au

[6] Recommendation 4 – Confidential information access and privacy training

- records of the content and participation by employees are kept
- is assessed annually to determine levels of retention and understanding of the content of the respective Information Privacy policy and supporting training material.

This follow-up report details how each agency has implemented the recommendations. We assess each recommendation and give an implementation status rating, as outlined in Figure 1A.

Figure 1A

Implementation status ratings

Rating	Description
Fully implemented	The agency has implemented the recommendation substantially or in its entirety.
Partially implemented	The agency has implemented part of the recommendation, but it has not fully satisfied the intent of the recommendation.
In progress	The agency has taken some action to implement the recommendation and efforts to complete implementation are ongoing.
Limited progress	The agency has taken minimal action to implement the recommendation and needs to make major efforts to complete it.

Source: Office of the Information Commissioner

2. Education and training as a risk mitigation strategy

Introduction

An effective privacy culture is essential to manage privacy and information security risks. Establishing robust privacy practices, procedures and systems involves:[7]

- considering functions that have greater risks because for example, they handle more sensitive information or use contractors, and implement appropriate processes for handling personal information throughout its lifecycle
- implementing processes that outline how staff should handle personal information in their daily duties and tailoring these processes to the agency
- implementing risk management processes to identify, assess and manage privacy and information security risks across the agency
- incorporating privacy and information security education into training programs at induction and at regular intervals during employment with the agency.

We expect that agencies consider privacy risks across their functions and use education and training as one strategy to mitigate the risks. When an agency does not have the assurance that its employees understand their privacy and information security obligations, it cannot demonstrate it has reasonably protected personal information against loss, unauthorised access, use, modification, or disclosure should a privacy breach occur.

In our original audit, we reported:

> *The three agencies have identified that educating and training their staff about information privacy and information security can mitigate their privacy and information security risks.*
>
> *However, they have not consistently mandated training on information privacy and information security at induction and at regular intervals during employment with the agency. This means that education and training are not as effective as they could be in mitigating risks.*

[7] Privacy management framework: enabling compliance and encouraging good practice – viewed at https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework#step-2-establish-robust-and-effective-privacy-practices-procedures-and-systems.

We made seven recommendations about education and training as a risk management strategy. Figures 2A and 2B show the implementation status of these recommendations.

Figure 2A

Department

Recommendation		Rating
1	within six months, mandates periodic refresher training on information privacy and information security for all employees.	Fully implemented
2	within six months, establishes a process that ensures new employees have read and understood at induction their duty of confidentiality under the *Communities Services Act 2007*.	Fully implemented

Source: Office of the Information Commissioner

Figure 2B

TAFE Queensland

Recommendation		Rating
3	within six months, implements its decision to mandate training on information privacy for all new employees.	Fully implemented
4	within six months, makes training about information security mandatory for all new employees.	Fully implemented
5	within six months, establishes a process that ensures new employees have read and understood at induction: • the policies, procedures and guidelines about information privacy and information security • their obligations of confidentiality under the *TAFE Queensland Act 2013*.	Fully implemented
6	within six months, mandates periodic refresher training on information privacy and information security for all employees.	Fully implemented
7	within twelve months, finalises, implements and educates all employees about its: • Information Security policy • Acceptable Use policy • Privacy of Personal Information guideline.	Fully implemented

Source: Office of the Information Commissioner

Results and conclusions

At the time of our original audit, the three audited agencies had either implemented or recognised the need for mandatory training at induction. But only the Public Trustee had planned to make regular refresher training mandatory.

Because no agency had consistently mandated staff training on information privacy and information security at induction and regular intervals, we concluded that their education and training was not fully effective as a risk mitigation strategy.

The agencies have now made it compulsory for their staff to complete training on information privacy and information security at induction and regular intervals. Mandatory refresher training increases the likelihood of employees retaining their awareness of information privacy and information security risks. It also makes education and training more effective as a risk management strategy.

The department

Recommendation 1

In 2018, we found that the department did not require existing staff to undertake regular information privacy and information security refresher training. However, the department delivered relevant training at the request of business units and could require specific staff to revisit training in response to a potential breach.

We recommended the department mandates periodic refresher training on information privacy and information security for all employees. In June 2019, the Director-General approved compulsory refresher training. All department staff must now complete an information privacy and information security refresher training every two years.

We assess the recommendation as fully implemented.

Recommendation 2

The department's employees are bound by confidentially obligations under the *Communities Services Act 2007*. Our original audit found the department did not ensure staff understood these obligations.

We recommended the department establishes a process that ensures new employees have read and understood at induction their duty of confidentiality under the *Communities Services Act 2007*.

The department has introduced a mandatory confidentiality obligations module in its induction package. This module clearly defines confidential information and the confidentiality obligations under the *Communities Services Act 2007*.

The module contains a quiz and requires employees to acknowledge they have read and understood the requirements.

We assess this recommendation as fully implemented.

TAFE Queensland

Recommendations 3 and 4

In 2018, we found that TAFE Queensland had not mandated information privacy and information security for new staff. Its voluntary information privacy module had a 10 per cent completion rate and TAFE Queensland did not have an information security induction module.

We recommended TAFE Queensland mandates information privacy and information security training for all new employees. TAFE Queensland has now included modules on information privacy and information security in its mandatory induction training package.

We assess these recommendations as fully implemented.

Recommendation 5

Our original audit found TAFE Queensland had policies and procedures relating to information privacy and information security, however, its training did not refer employees to these documents.

We recommended TAFE Queensland establishes a process that ensures new employees have read and understood the policies, procedures and guidelines about information privacy and information security at induction.

While TAFE Queensland does not specifically require employees to read these documents at induction, the mandatory induction training covers key content from the information security and information privacy documents. The privacy training module outlines the confidentiality obligations under the *TAFE Queensland Act 2013*.

This is a satisfactory alternative.

Only the information security training module contains an assessment. The information privacy training module does not assess whether staff have understood the training content and their obligations. TAFE Queensland advised it is in the process of enhancing embedded quizzes to test understanding throughout its induction and refresher training.

Using assessments increases the likelihood of employees understanding training content. It also gives agencies greater assurance that staff are aware of their obligations and enhances the effectiveness of training as a risk mitigation strategy.

We assess the recommendation as fully implemented.

Recommendation 6

In 2018, we found that TAFE Queensland did not require existing staff to periodically refresh their information privacy and information security training. We recommended TAFE Queensland mandates periodic refresher training on information privacy and information security for all staff.

All TAFE Queensland employees must now undertake information privacy and security refresher training in January every year.

We assess the recommendation as fully implemented.

Recommendation 7

At the time of our original audit, TAFE Queensland had drafted an Information Security policy, an Acceptable Use policy and a Privacy of Personal Information guideline. We recommended TAFE Queensland finalises and implements these documents. We also recommended it educates all employees about the documents.

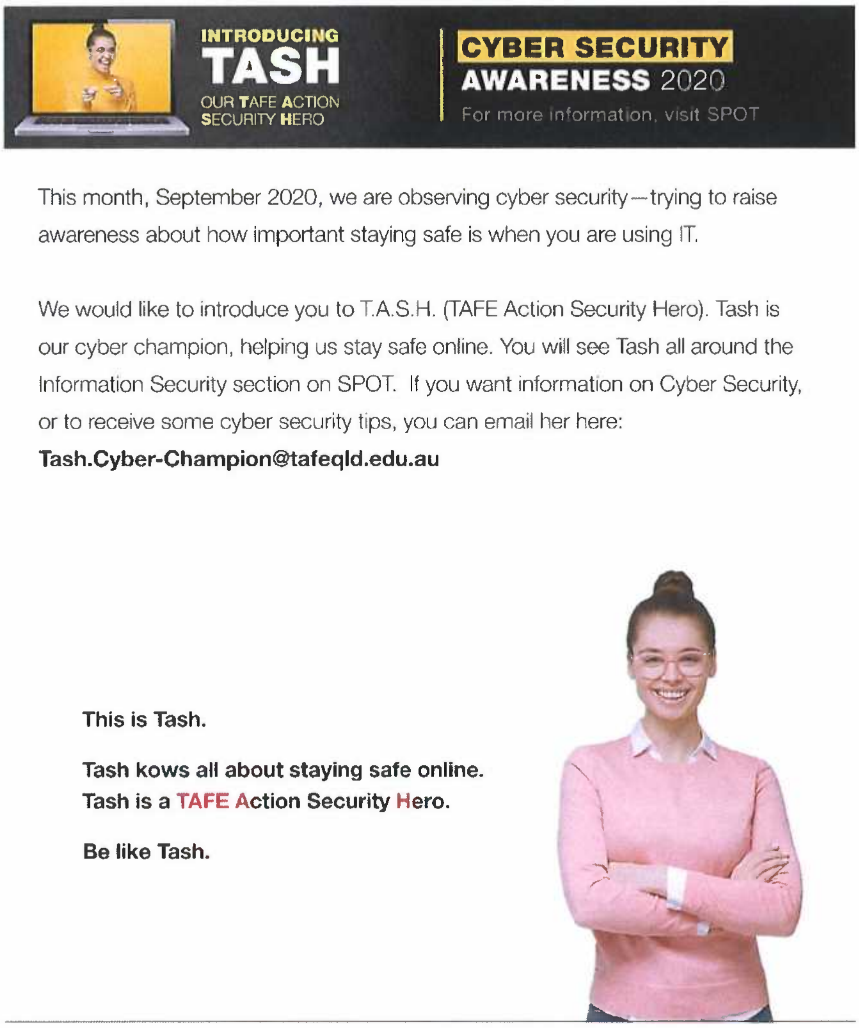
The three documents are now in effect and they cover relevant aspects of managing privacy risks. TAFE Queensland has incorporated key elements of these documents in its mandatory refresher training for all staff. This approach adequately educates employees about policy content.

We assess the recommendation as fully implemented.

TAFE Queensland has taken additional steps to inform employees about these policies, such as all-staff emails and intranet campaigns. For example, as part of its 2020 cyber security awareness campaign, it developed a virtual cyber security champion, ‘TASH’, promoting information security on various online channels.

Figure 2C

TAFE Queensland – TASH



INTRODUCING
TASH
OUR TAFE ACTION
SECURITY HERO

CYBER SECURITY
AWARENESS 2020
For more information, visit SPOT

This month, September 2020, we are observing cyber security—trying to raise awareness about how important staying safe is when you are using IT.

We would like to introduce you to T.A.S.H. (TAFE Action Security Hero). Tash is our cyber champion, helping us stay safe online. You will see Tash all around the Information Security section on SPOT. If you want information on Cyber Security, or to receive some cyber security tips, you can email her here:
Tash.Cyber-Champion@tafeqld.edu.au

This is Tash.

Tash kows all about staying safe online.
Tash is a TAFE Action Security Hero.

Be like Tash.

Source: TAFE Queensland

3. Training material

Introduction

For training to be effective, it must be comprehensive, accurate and relevant to the context of the agency. Agencies can adopt tailored training packages specific to their work, or supplement general information privacy and security training with agency specific training.

Training should include practical scenarios that demonstrate how to apply information privacy and information security principles in their day-to-day duties. The Crime and Corruption Commission's *Operation Impala: Report on misuse of confidential information in the Queensland public sector report*, outlines some benefits of using real-life scenarios and de-identified case studies as part of the training.

We expect that agencies' information privacy and information security training material:

- covers all relevant elements of information privacy and information security
- is accurate and consistent with the *Information Privacy Act 2009* and other resources
- is tailored to meet the needs of the agency.

We made three recommendations about training material. Figures 3A, 3B and 3C show the implementation status of these recommendations.

Figure 3A

Public Trustee

Recommendation		Rating
8	within three months, supplements its information privacy training with the contents of its Information Privacy Plan.	Fully implemented

Source: Office of the Information Commissioner

Figure 3B

Department

Recommendation		Rating
9	within six months, complements its general information privacy training with practical examples and scenarios tailored to its context.	Fully implemented

Source: Office of the Information Commissioner

Figure 3C

TAFE Queensland

Recommendation		Rating
10	within twelve months, incorporates relevant components of information security from its policies and procedures into its information security awareness training.	Fully implemented

Source: Office of the Information Commissioner

Results and conclusions

In our original audit we reported that the information privacy training material of the three audited agencies was consistent with the *Information Privacy Act 2009*. However, we noted each agency could improve the content of its information privacy and/or information security training material.

The Public Trustee and TAFE Queensland have now updated their information privacy and information security training to better reflect their policies and procedures. The department has also updated its privacy training to include practical scenarios.

Comprehensive, relevant and practical training content means employees are more aware of the privacy and information security risks. This increases the effectiveness of training and education as a risk mitigation strategy.

The Public Trustee

Recommendation 8

In 2018, we noted the Public Trustee had an Information Privacy Plan. We recommended the Public Trustee supplements its information privacy training module with content from the plan.

The training module now reflects the content of the Information Privacy Plan. It includes examples of the types of personal information the agency collects, and how the Information Privacy Principles apply to the collection, use and disclosure of personal information.

Generally, the Public Trustee's information privacy training is clear and detailed. It covers relevant aspects of the *Information Privacy Act 2009* in sufficient depth for an induction course. The training could be further improved with practical, scenario-style examples or assessment questions.

We assess the recommendation as fully implemented.

The department

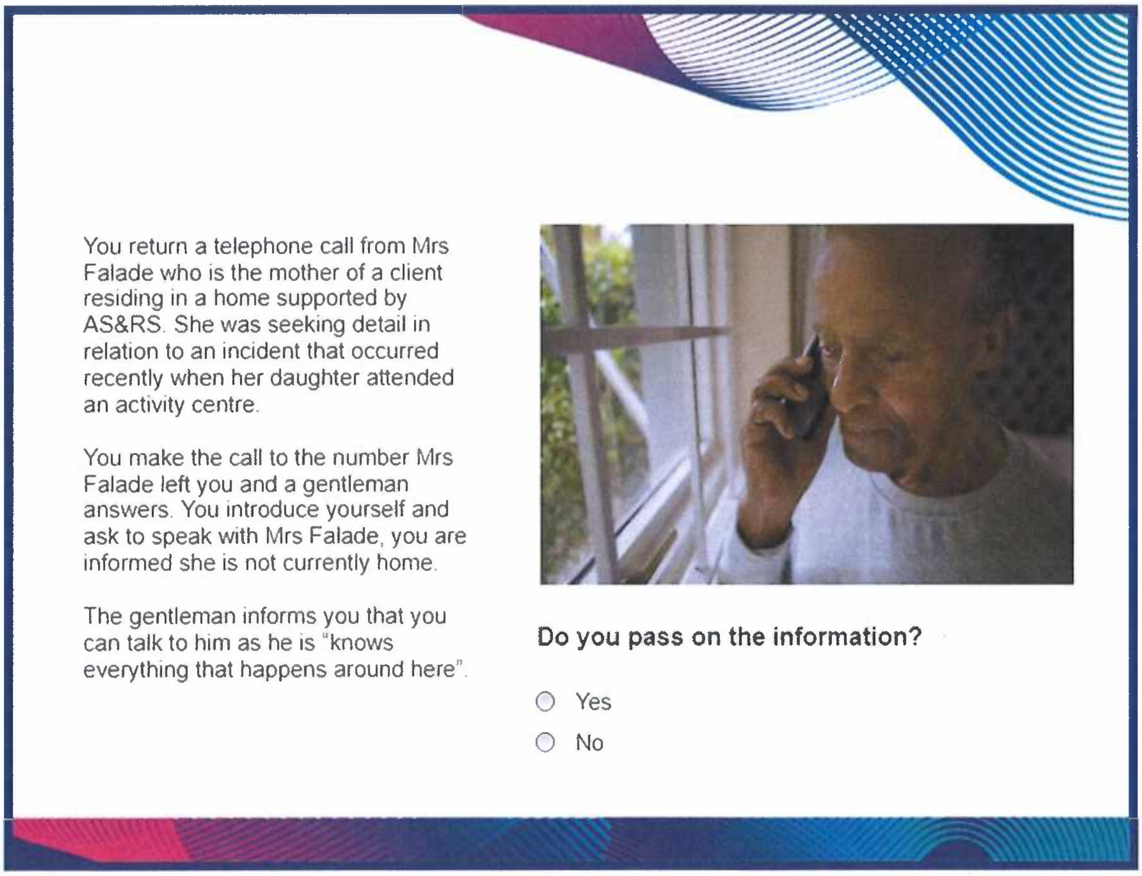
Recommendation 9

Our original audit found the department had generally good information privacy training. However, we recommended the department complements this training with practical examples and scenarios tailored to its context.

The department has incorporated scenarios to its information privacy training. The scenarios are detailed and specific to the work of the department. They cover a wide range of situations, including collecting, using and disclosing personal information. One example is provided below.

Figure 3D

Practical scenario



You return a telephone call from Mrs Falade who is the mother of a client residing in a home supported by AS&RS. She was seeking detail in relation to an incident that occurred recently when her daughter attended an activity centre.

You make the call to the number Mrs Falade left you and a gentleman answers. You introduce yourself and ask to speak with Mrs Falade, you are informed she is not currently home.

The gentleman informs you that you can talk to him as he is "knows everything that happens around here".

Do you pass on the information?

○ Yes

○ No

Source: Department of Seniors, Disability Services and Aboriginal and Torres Strait Islander Partnerships

Many examples include a quiz, prompting employees to consider the correct course of action. This increases the likelihood of employees understanding and applying the Information Privacy Principles in their regular work.

The department has taken additional steps to provide agency specific information to employees. In the leadup to Privacy Awareness Week in 2019, it published a series of short 'did you know' articles on its intranet home page.

The articles included practical privacy topics, such as misdirected emails, shredding documents, floor security and privacy impact assessments. This type of campaign is an effective way to remind employees of their privacy obligations and reinforce appropriate privacy behaviours in their everyday work.

In response to COVID-19, the department issued further practical privacy guidance to employees about working from home. This includes having sensitive conversations away from smart home devices (such as Siri, Alexa or Google Home), locking IT devices when not in use, and the appropriate use of IT systems.

We assess the recommendation as fully implemented.

TAFE Queensland

Recommendation 10

In 2018, we found TAFE Queensland’s training on information security missed key components and did not reflect important aspects of its policies.

We recommended TAFE Queensland incorporates relevant components of its information security policies and procedures in its security awareness training. This included content on employee responsibilities and the acceptable use of information.

TAFE Queensland has updated its training material on information security.

The induction training adequately captures key features of the policy and details an employee’s responsibilities. It outlines how to classify and handle information.

Further, the induction training contains practical references, including six Department of Defence videos on information security risks, including passwords, foreign devices, public Wi-Fi and phishing.

TAFE Queensland's mandatory refresher training adequately captures key elements of the information security policy, including safeguarding user ID and passwords.

We assess the recommendation as fully implemented.

4. Enrolment and monitoring systems and processes

Introduction

When a very high proportion of staff complete the education and training, it reinforces an agency's privacy culture and reduces the likelihood of privacy and information security risks materialising.

For agencies to deliver training effectively, their systems and processes must:

- enrol all eligible employees in the relevant training modules
- identify and follow up employees who do not complete the training within the prescribed period.

Our original audit examined whether the agencies had effective systems and processes to ensure all eligible employees complete the information privacy and information security modules.

We made two recommendations about enrolment and monitoring systems and processes.

Figure 4A
Department

Recommendation		Rating
11	within six months, implements more robust systems and procedures to ensure all employees complete the mandatory training on information privacy and information security when due.	Fully implemented

Source: Office of the Information Commissioner

Figure 4B
TAFE Queensland

Recommendation		Rating
12	within twelve months implements systems and procedures to ensure all employees complete the mandatory training on information privacy and information security when due.	Fully implemented

Source: Office of the Information Commissioner

Results and conclusions

In our original audit, the Public Trustee and the department had established processes for monitoring the completion of information privacy and information security training. However, their systems did not ensure new staff completed the mandatory training within the prescribed timeframe, in part because reminder emails were sent to employees but not their supervisors.

We noted that the Public Trustee had planned to implement a new learning management system in 2019.

A large proportion the department's workforce, such as Residential Care Officers, did not have access to the ICT network. The department delivered face-to-face training to these staff and recorded their attendance in the system.

TAFE Queensland did not monitor information privacy training completion. The low completion rates at the time reflected the optional nature of the training.

Both the department and TAFE Queensland have improved their enrolment and monitoring systems and process. This increased the proportion of staff completing the training.

The department

Recommendation 11

In 2018, we found that the department had a devolved process for checking that new staff complete the mandatory induction modules. Course content owners, such as the department's Information Privacy unit or the Information Services branch, were responsible for following up on course completions. The department was achieving completion rates above 80 percent for induction modules. At the time it did not require existing staff to undertake regular information privacy and information security refresher training.

We recommended the department implements more robust systems and procedures to ensure all employees complete the mandatory training on information privacy and information security when due.

The department now has a process that automatically enrols employees and prompts users to complete training when due (including non-network employees). Individual managers are copied into reminder emails sent to staff.

Senior executives receive quarterly strategic reports on training completion in their areas. The department also provides detailed completion reports to business areas to follow up incomplete training with individual employees.

As at December 2020, 81.7 per cent of departmental staff had completed information privacy training and 76.2 per cent had completed information security training, whether at induction for new starters or the mandatory refresher for existing staff. The department has a large cohort of staff in frontline roles, such as the Residential Care Officers. Due to the nature of their role, they are rostered to 24-hour shifts, 7 days a week. They are largely on shift by themselves, supporting people with their personal and sometimes complex care needs and daily living. As these staff do not have ongoing access to the IT network, the department has other methods to deliver training, like face-to-face or self-paced workbooks.

The department advised that the COVID-19 pandemic affected the training for these staff and consequently the overall completion rates. Education on COVID-safe practices was prioritised, including training on the use of personal protective equipment. There were also additional restrictions in disability accommodation, including on people visiting the workplace.

Despite the challenges, about three quarters of Disability Accommodation Respite and Forensic Services staff completed the information privacy and information security training.

The department advised it is committed to have all its staff completing the training including the refresher training and has set a target of over 90 per cent. Although the completion rates being below target, we assess this recommendation as fully implemented in recognition of the exceptional circumstances of 2020.

TAFE Queensland

Recommendation 12

Our original audit found TAFE Queensland's information privacy training was optional for all staff. As a result, only 16.5 per cent of staff completed privacy training on induction. TAFE Queensland did not require formal refresher training.

We recommended TAFE Queensland implements systems and procedures to ensure all employees complete mandatory training on information privacy and security when due.

TAFE Queensland now uses a central learning management system to administer staff training. This system automatically prompts users to complete their training and produces quarterly completion reports for management.

Regional human resource teams are responsible for generating compliance reports and forwarding these to individual managers where necessary. Managers are responsible for following up outstanding training with employees.

TAFE Queensland achieved a very high completion rate in 2020, with 95 per cent of new starters completing the mandatory induction training and 96 per cent of staff completing the mandatory refresher training.

We assess the recommendation as fully implemented.

5. Appendix

In accordance with our policies and procedures, we provided this report to the Public Trustee of Queensland, the Department of Seniors, Disability Services and Aboriginal and Torres Strait Islander Partnerships and TAFE Queensland with a request for comment.

Queensland
Government

Department of
Seniors, Disability Services and Aboriginal and Torres Strait Islander Partnerships

Our reference: 01040-2021

11 March 2021

Ms Rachael Rangihaeata
Information Commissioner
PO Box 10143
Adelaide Street
BRISBANE QLD 4000
audit@oic.qld.gov.au

Dear Ms Rangihaeata

Thank you for your letter of 25 February 2021 providing the opportunity to comment on the follow-up audit into the Department of Seniors, Disability Services and Aboriginal and Torres Strait Islander Partnerships' (the department) implementation of the recommendations in Report No. 1 for 2018–19. I note that all recommendations were assessed as fully implemented.

I would like to initially acknowledge the important role and trust that the community provides to the department in ensuring their personal information is managed sensitively, appropriately, and safely.

Information privacy and information security training has been a key strategy for building staff capability and in assisting them to understand their role, their obligations, and expectations. This review has been a valuable opportunity for the department to further improve the training, practices, and systems in place, and most importantly, provide our frontline staff with more practical examples that are meaningful for them on a day to day basis.

The report is fully supported, and I have no additional comments to make.

I would also like to thank your staff for their assistance and guidance through the audit.

If you require further information, I encourage you to contact Ms Belinda Huig, Manager, Human Resources and Ethical Standards, Department of Seniors, Disability Services and Aboriginal and Torres Strait Islander Partnerships on 30978558 or by email at Belinda.Huig@communities.qld.gov.au.

Yours sincerely

Dr Chris Sarra
Director-General

444 Queen Street Brisbane Qld 4000
GPO Box 1449 Brisbane Qld 4001

SINCE Public Trustee 1916

For reply please *quote: JGIS&G - T21/256 - D21/6829*

15 March 2021

Ms Rachael Rangihaeata
Information Commissioner
Office of the Information Commissioner
PO Box 10143
Adelaide Street
BRISBANE QLD 4000

Dear Ms Rangihaeata

Follow-up audit - awareness of privacy obligations

Thank you for your letter of 25 February 2021, enclosing a copy of the Follow-up of Report No.I for 2018-19 (Report No.3 for 2020-21).

I have considered the further observations in the Follow-up of Report No. 1 and appreciate your suggestions to further enhance the information privacy training provided to Public Trustee. I would like to confirm that the Public Trustee will implement your suggestion and is in the process of adding practical scenario-style examples and assessment questions in its information privacy mandatory training course.

I have no further comments on the proposed report.

Thank you for the opportunity to respond. If my office can assist with any further information, please contact Ms Josephine Giles, Senior Director Governance and Risk on 07 3564 2086.

Yours sincerely

Samay Zhouand
Acting Public Trustee of Queensland and CEO

tafe
Queensland

1 2·MAR 2021

Ms Rachael Rangihaeata
Information Commissioner
PO Box 10143
Adelaide Street
BRISBANE OLD 4000

Dear Ms Rangihaeata

Thank you for your letter dated 25 February 2021 regarding the follow-up audit in relation to TAFE Queensland's implementation of the recommendations from Report No. 1 for 2018-19 - Awareness of privacy obligations.

I acknowledge your proposed Report to Parliament and I thank you for the opportunity to respond. TAFE Queensland has no issues with the content of the report and its findings as they relate to TAFE Queensland.

I commend your auditors for how they conducted the audit and their engagement with our staff. Their approach was very professional and considerate of the workload of the involved staff members. It was also very constructive, resulting in improvements in how TAFE Queensland engages staff in understanding and delivering against their privacy obligations.

If any further information or follow up is required, please do not hesitate to contact either myself or the TAFE Queensland Chief Information Officer, Mr Alan Chapman, on telephone 3514 3764 or via email at Alan.Chapman@tafeqld.edu.au.

Yours sincerely

MCampbell

Mary Campbell
Chief Executive Officer
TAFE Queensland

Ref: TQ21/9347