Awareness of privacy obligations

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

Report No. 1 to the Queensland Legislative Assembly for 2018-19

We thank the staff of the audited agencies for their support and cooperation.

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
Email administration@oic.qld.gov.au
Web www.oic.qld.gov.au

ISBN: 978-0-6484026-0-2

December 2018

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

Dear Mister Speaker

I am pleased to present *Awareness of privacy obligations: How three Queensland government agencies educate and train their employees about their privacy obligations*. We prepared this report under section 135 of the *Information Privacy Act 2009*.

The report outlines agencies' practices in educating and training employees about information privacy and information security. In particular, we examined whether the training material covers information privacy adequately and the processes support timely completion of the training. The report identifies examples of good practice and makes recommendations to all government agencies.

In accordance with subsection 193(5) of the Act, I request that you arrange for the report to be tabled in the Legislative Assembly on the next sitting day.

Yours sincerely

Rachael Rangihaeata
Information Commissioner

Table of contents

1 Summary

The inadvertent or deliberate disclosure of personal information can have serious consequences for the individual whose privacy the agency breached, the agency concerned and the employee.

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

One mitigation strategy agencies can adopt is to train and educate their employees about information privacy and information security obligations and expectations. To be effective, training and education activities should be regular, comprehensive, accurate and tailored to the context of each agency. There should also be systems and processes in place to ensure all employees complete mandatory training when due.

The objective of the audit was to determine whether agencies educate and train their employees about their obligations under the *Information Privacy Act 2009* appropriately. We considered whether three government agencies - the Public Trust Office (**the Public Trustee**), the Department of Communities, Disability Services and Seniors (**the department**) and TAFE Queensland:

- 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.

Conclusions

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.

It is encouraging to note that the agencies identified some of these issues before our audit and explored ways to make the training more effective. For example, at the time of our audit, all agencies had either implemented (the Public Trustee, the department) or recognised the need

for (TAFE Queensland) mandatory training on information privacy and information security at induction.

The content of the agencies' training on information privacy is accurate but does not always include all the elements necessary for employees to understand their obligations under the *Information Privacy Act 2009*. While useful to raise general awareness, the training on information privacy for the department and the Public Trustee should include scenarios that illustrate how the Act applies in the agency's context. Similarly, TAFE Queensland has the opportunity to adopt comprehensive training content on information security, as it restructures into one single entity.

The agencies also run various awareness campaigns or issue agency-wide messages about information privacy and security. These are useful reminders. But when existing staff do not go through a mandatory, periodic refresher training, their understanding of privacy and security obligations could fade over time.

The training completion rates for the three agencies show that their processes or systems for ensuring that employees complete the relevant training modules within the prescribed period are not always effective.

Key findings

Agencies should consider the privacy risks of their various functions and identify education and training as a risk mitigation strategy. Information security training complements the training on information privacy. It makes employees aware of potential threats to the agency's information so they can then better protect it against unauthorised access, loss, misuse and disclosure. Training can be formal or informal. Other awareness activities remind staff of their privacy and information security obligations.

The three agencies use education and training as a risk mitigation strategy. However, they have not consistently, for the period audited[1], mandated training on information privacy and information security at induction or at regular intervals during employment with the agency.

Figure 1

	Department	**Public Trustee**	**TAFE Queensland**
Information privacy training mandatory at induction	Yes	Yes	Identifed but not yet implemented
Information security training mandatory at induction	Yes	Yes	Identified but limited in scope
Information privacy training mandatory periodical refresher	No	Identified and implemented during audit	No
Information security training mandatory periodical refresher	No	Yes	No

Source: Office of the Information Commissioner

[1]For staff commencing or employed between 1 July 2016 to 31 December 2017

At the time of our audit, the agencies had either implemented or recognised the need for mandatory training on information privacy and security at induction. But only the Public Trustee had planned to make regular refresher training mandatory.

The Public Trustee has an established process to ensure staff know about the secrecy obligations under the *Public Trustee Act 1978*. The department and TAFE Queensland also have duty of confidentiality provisions in their respective enabling legislation. However, they cannot demonstrate that their staff are aware of the provisions or understand them.

For training to be effective as a risk mitigation strategy, the content must be comprehensive, accurate and relevant to the context of the agency. Practical scenarios and revision questions should relate to the employee's functions and demonstrate how to apply information privacy and security when undertaking their duties. Agencies can adopt tailored training packages specific to their functions, or supplement general information privacy and security training with agency specific training.

The three agencies have adopted information privacy training modules that are accurate and consistent with the *Information Privacy Act 2009*. During the audit, the Public Trustee amended its information privacy module. It further intends to include elements of its Information Privacy Plan in the training module. The department's training module, while robust, does not include enough agency specific examples that illustrate in a practical way how the Act and the privacy principles apply in an employee's day-to-day role.

The information security training of the Public Trustee and the department is comprehensive. The modules meet their needs in raising staff awareness of potential security threats to information assets.

TAFE Queensland's current training on information security is missing key components of information security. There are policies, some of them in draft, that cover most of the missing aspects of information security. While the policies outline TAFE Queensland's commitment to mitigating information risks, they are not part of a structured training module on information security. The agency's induction process ensures employees are aware of where to find these policies, however it does not require employees to acknowledge that they have read and understood them. This means that TAFE Queensland cannot be sure all staff are familiar with their information security obligations.

Adopting comprehensive training content is not enough; employees need to actually complete the training. Thus, agencies must have enrolment and monitoring systems and processes that:

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

The Public Trustee and the department have established processes for enrolling staff in, and monitoring completion of, the information privacy and information security training modules. While the Public Trustee achieves a high completion rate, its current process does not support timely completion of training. Its new learning management system should see more staff

completing their training within the specified timeframe. The training completion rates for the department indicate that its process for ensuring staff enrol and complete the relevant training modules is not always effective.

The learning management system of TAFE Queensland can monitor whether employees complete their training. However, the agency has not activated this functionality for the training module on information privacy. The low completion rate for the audited period reflects the optional nature of the training at the time. TAFE Queensland identified this issue shortly before our audit and decided to include information privacy in its program of mandatory training at induction.

Recommendations

We recommend that the:

Department of Communities, Disability Services and Seniors

1. within six months, mandates periodic refresher training on information privacy and information security for all employees.
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*.
9. within six months, complements its general information privacy training with practical examples and scenarios tailored to its context.
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.

TAFE Queensland

3. within six months, implements its decision to mandate training on information privacy for all new employees.
4. within six months, makes training about information security mandatory for all new employees.
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*.
6. within six months, mandates periodic refresher training on information privacy and information security for all employees.

7. within twelve months, finalises, implements and educates all employees about its:
    - Information Security policy
    - Acceptable Use policy
    - Privacy of Personal Information guideline.
10. within twelve months, incorporates relevant components of information security from its policies and procedures into its information security awareness training.
12. within twelve months implements systems and procedures to ensure all employees complete the mandatory training on information privacy and information security when due.

Public Trustee

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

We also recommend that all agencies:

a. include information privacy and information security training in their **mandatory induction process** for all employees.
b. **mandate periodic refresher training** on information privacy and information security for all employees.
c. ensure the **training content** on information privacy and information security is comprehensive, contemporary and tailored to the agency's context.
d. implement systems and procedures to ensure all employees complete mandatory training on information privacy and information security when due.

Note: 'All agencies' means all government agencies subject to the *Information Privacy Act 2009* including Queensland Government departments, statutory bodies, local governments, public universities, Hospitals and Health Services, and other public authorities.

Agency responses

We provided a copy of this report to the audited agencies for their comments. We have considered their views in reaching our conclusions.

The agencies' responses are in Appendix A.

2 Context

In its Notifiable Data Breaches Quarterly Statistics Report issued on 30 October 2018, the Office of the Australian Information Commissioner said that 37 per cent of breaches reported were due to human error. They resulted from:

- insecurely disposing of information
- losing paper work or data storage devices
- sending personal information to the wrong recipient
- disclosing information without appropriate authority.

The report also identified that 57 per cent of reportable data breaches happen because of malicious or criminal attack. This type of breach includes:

- cyber incidents such as phishing, hacking, malware and brute force attack
- insider threats like a rogue employee
- theft of paperwork or data storage devices.

Malicious or criminal attacks are deliberate attempts to exploit known vulnerabilities for financial or other gain. However, the Office of the Australian Information Commissioner noted that cyber incidents also exploit vulnerabilities involving a human factor, such as clicking on phishing emails or disclosing passwords. When publishing the quarterly statistical report, the Australian Information Commissioner said that

"…training staff on how to identify and prevent privacy risks needs to be part of business as usual."

Contact information, such as a person's name, home address, email address or phone number, was the most common type of personal information involved in a breach.

Whether it is the result of a human error or a malicious attack, the inadvertent or deliberate disclosure of personal information can have serious consequences for the individual whose privacy has been breached, the organisation and the employee responsible for the breach. Individuals may suffer discrimination, embarrassment, financial or even physical and psychological harm. The organisation may experience reputational damage and loss of public trust and confidence in its ability to protect personal information. Employees may be subject to disciplinary action such as termination of employment.

Queensland government agencies collect and handle personal information of various sensitivities in delivering their services to the community. The public entrusts these agencies with their personal information.

The *Information Privacy Act 2009* provides safeguards for handling personal information in the public sector environment. Government agencies, and their employees, must comply with the Act and the privacy principles.[2]

Under Information Privacy Principle 4, an agency must protect documents containing personal information against loss, and unauthorised access, use, modification or disclosure, and any other misuse. Protection must include security safeguards adequate to provide the level of protection that can reasonably be expected to be provided.

Information security risks arise from threats to the agency's physical and operational controls protecting its data. They are internal and external to the agency and include:

- human behaviour such as carelessly handling data, sharing passwords, downloading infected attachments or discussing sensitive information in an open environment
- phishing and other unsolicited emails designed to obtain access to personal information
- ineffective physical and technical internal controls to keep personal information secure.

Agencies failing to appropriately address information security risks increase their exposure to privacy risks.

The likelihood and impact of privacy risks varies between job roles and functions. For example, job roles and functions where employees who regularly interact with the public and have access to highly personal information such as health records, present higher privacy risks than roles where staff have limited public interaction or which do not involve personal information. Similarly, roles where employees handle large data sets containing personal information present higher risks than where staff have access to small amounts of personal information of a limited number of individuals. It is up to each agency to assess these risks and establish strategies to mitigate them.

One mitigation strategy agencies can adopt is to train and educate their employees about information privacy and information security obligations and expectations. For example:

- formally training all employees about the *Information Privacy Act 2009* and information security
- ensuring all employees know about the confidentiality or secrecy provisions in the agency's enabling legislation
- reinforcing and reminding employees of their privacy and information security obligations through general awareness activities.

Agencies can adopt tailored training packages specific to their work, or supplement general information privacy and security training with agency specific training. As part of our suite of online courses, we offer a general awareness module on the *Information Privacy Act 2009*. Agencies can access our training, courses and learning management system free of charge. The system allows an agency to monitor and report on participants' progress. Alternatively, an

[2] Chapter 2, see in particular sections 26 and 27, and Schedule 3 of the *Information Privacy Act 2009* (Qld). Health agencies must comply with the National Privacy Principles, under sections 30 and 31, and Schedule 4 of the *Information Privacy Act 2009* (Qld).

agency can provide its staff with access to our courses through its learning management system for a fee.

Audit objective and scope

The objective of the audit was to determine whether agencies educate and train their employees about their obligations under the *Information Privacy Act 2009* appropriately.

The audit assessed whether:

- agencies' education and training material covers information privacy adequately
- agencies educate and train their employees about information privacy.

In this audit, 'employees' means permanent, temporary and casual employees, whether employed full-time or part-time.

We conducted this audit under section 135 of the *Information Privacy Act 2009,* which allows the Information Commissioner to conduct:

> *reviews into personal information handling practices, including technologies, programs, policies and procedures, to identify privacy related issues of a systemic nature generally*

and to comment on:

> *any issues relating to the administration of privacy in the public sector environment.*

Appendix B contains the details of the audit methodology.

Scope

The audit examined three government agencies that employ permanent, temporary and casual staff:

- The Public Trustee
- Department of Communities, Disability Services and Seniors
- TAFE Queensland.

The audit did not examine the education and training content that does not relate to information privacy or confidentiality. The audit did not examine the education and training the agencies give to other types of employees or contingent workforce (volunteers, contractors, consultants, or others).

The Public Trustee

The Public Trustee has been serving Queensland since 1916. Originally established as the Public Curator, the Public Trustee has grown to be Australia's largest public trustee organisation.

It operates under the *Public Trustee Act 1978* and its functions include:

- preparing wills for distributing estate assets
- providing executor services in administering deceased estates
- preparing enduring powers of attorney and acting as an impartial attorney on financial matters
- managing the financial affairs for clients with impaired decision-making, including a service to examine the accounts of private administrators acting as financial attorneys for clients
- selling and auctioning client properties
- acting as the nominated trustee of client trusts including philanthropic foundations.

The personal information the Public Trustee collects and holds about a client depends on the service it supplies. For example, the Deceased Estates and Financial Management work groups may hold highly personal and sensitive information such as health records and medical reports, details of assets and liabilities, and certificates of birth, death or marriage.

The Public Trustee operates throughout Queensland. It is present in 15 locations and offers services through the Queensland Government Agent Program and local court network.[3]

As at 30 June 2018, the Public Trustee employed 620 staff.[4] Its workforce consisted of 530 permanent (85%), 85 temporary (14%) and 5 contracted (1%) staff.

[3] The Public Trustee Annual Report 2016-17.
[4] MOHRI Quarterly Report June 2018.

Department of Communities, Disability Services and Seniors

The Department of Communities, Disability Services and Seniors is the lead Queensland Government agency coordinating the State's transition to the National Disability Insurance Scheme (**NDIS**).

The machinery of government changes in December 2017 have also significantly changed the department's functions and services to the community. The priorities for the department over this term of Government include to:[5]

- ensure effective community recovery capability is in place to respond to natural disasters
- work with key stakeholders to improve the quality of community services in Queensland
- continue to contribute to the Government's child and family reform agenda
- assist older people in leading healthy and productive lives and ensure Government policies and programs continue to be age friendly.

The department delivers these priorities through the following functions and services:

- Community services, including support services for carers and vulnerable members of the community, and community recovery for people affected by disasters
- Disability services, including support services for people with a disability, their families and carers, Accommodation Support and Respite Services and Community Care Services
- Seniors, including support services for older people including seniors' cards, concessions, social connection programs legal and support services.

The department operates a network of 17 community services regional offices and 16 disability services regional offices across Queensland.

As at 30 June 2018, the department employed 2,751 staff. Its workforce consisted of 2,119 permanent (77%), 350 temporary (13%), 266 casual (9%) and 16 contract staff (1%).[6] The largest component of the department's workforce is in Accommodation Support and Respite Services, a registered NDIS service provider.

[5] Ministerial Charter Letters: Coralee O'Rourke MP – Minister for Communities and Minister for Disability Services and Seniors: viewed at https://www.cabinet.qld.gov.au/ministers/charter-letters.aspx.
[6] MOHRI Quarterly Report June 2018.

TAFE Queensland

The *TAFE Queensland Act 2013* established TAFE Queensland as a statutory body on 1 July 2014. The legislation defines the objectives and functions associated with TAFE Queensland. Under the Act, TAFE Queensland:

- provides vocational education and training services
- provides further education to support and complement vocational education and training services
- produces and sells vocational education and training products
- engages with industry on matters relating to its vocational education and training services.

In July 2013, TAFE Queensland began amalgamating all TAFE institutes across the state into six regional registered training organisations. In July 2017, TAFE Queensland underwent further structural change and commenced consolidating the six registered training organisations into a single agency to provide more practical, industry-led training across the state more effectively and efficiently.

The Queensland Government's objectives for TAFE Queensland are to contribute to the community through skills development that align with industry requirements and increase job opportunities for students. In meeting the Government's objectives, TAFE Queensland delivers training across a range of industries from entry-level certificates to bachelor degrees.[7]

TAFE Queensland is now one of Australia's largest education providers. In 2017-18, it educated and trained approximately 121,000 students throughout Australia and overseas.[8]

As at 30 June 2018, TAFE Queensland employed 4,666 staff. Its workforce consisted of 2,833 permanent (61%), 1,136 temporary (24%), 579 casual (12%) and 118 contract staff (3%)[9] across 50 TAFE locations throughout Queensland.

[7] Viewed at https://tafeqld.edu.au/about-us/who-we-are/index.html on 17 July 2018.
[8] TAFE Queensland Annual Report 2017-2018.
[9] MOHRI Quarterly Report June 2018.

Report structure

The report is structured as follows:

Section	Contents
Chapter 1	executive summary of our key findings, conclusions and audit recommendations
Chapter 2	discusses privacy and information security risks and audit objectives and scope
Chapter 3	examines education and training as a tool for mitigating privacy risks
Chapter 4	discusses the content of the training material
Chapter 5	analyses how effectively agencies deliver information privacy and information security training to staff
Appendix A	contains the responses received from the audited agencies
Appendix B	outlines the audit methodology

3 Education and training as a risk mitigation strategy

Building and maintaining a good privacy and information security culture within an agency is essential in minimising privacy and information security risks. The Office of the Australian Information Commissioner notes that establishing robust privacy practices, procedures and systems[10] involves a number of actions, including:

- 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 have to 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 have considered the privacy risks of their various functions and have identified education and training as a risk mitigation strategy.

Information security training complements training on information privacy. It makes employees aware of potential threats to the agency's information so they can then better protect that information against loss, unauthorised access, use, modification or disclosure, and any other misuse.

Training can be formal or informal. Other awareness activities can also remind staff of their privacy and information security obligations.

Conclusion

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.

At the time of our audit, the 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. While other, informal awareness activities or communications are useful reminders, the lack of systematic, periodic refresher training for all staff about information

[10] 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.

privacy and information security means their understanding of privacy and security obligations could fade over time.

Detailed findings

The three audited agencies have adopted strategies to mitigate their information risks, although they have not formally documented the privacy risks of their various functions. The strategies include education and training on information privacy and information security.

Information privacy

The Public Trustee and TAFE Queensland give their respective employees the same information privacy training regardless of their position, employment type or location. Most staff at the department receive the same general privacy training. The department also delivers specialised information privacy training to relevant teams and programs, such as Residential Care Officers within Accommodation, Support and Respite Services.

The three agencies set mandatory training on information privacy at induction for all new employees, although this is a recent development at TAFE Queensland.

The Public Trustee includes information privacy in its mandatory induction program. New staff have three months to complete the information privacy module.

In 2016-17, an internal audit at the Public Trustee examined the agency's maturity and compliance with the *Information Privacy Act 2009* and the *Right to Information Act 2009*. It recommended the Public Trustee makes information privacy training a mandatory component of its staff annual reinforcement training. The Public Trustee accepted the recommendation and committed to implement it by 30 June 2017.

At the commencement of our audit, the Public Trustee had not yet implemented internal audit's recommendation. Changes to key personnel within the agency, and the agency's decision to await the outcome of this audit, delayed implementation. In October 2018, the Public Trustee updated its induction material. It also included information privacy in the Mandatory Compliance Program as a core course module that employees must revisit annually.

From February 2019, the Public Trustee will release the information privacy module for existing staff to complete within 20 business days. This brings training on privacy in line with the information security module all employees must complete annually.

The department's new employees must undertake information privacy training at induction. They have 30 days to complete the training. The department does not require its existing staff to revisit information privacy training periodically throughout their employment. However, it delivers relevant training at the request of business units. It also may require specific staff to revisit training in response to an incident or potential breach.

In 2017, the department's Information Privacy team considered introducing refresher training on information privacy and a new, agency-specific training module. However, it put the review on hold because of machinery of government changes.

The regions of TAFE Queensland have their own procedures outlining the induction process for new employees. The procedure for SkillsTech sets out the mandatory induction that employees must complete. The procedure does not specify which online modules new employees must complete from the eight modules available on the SkillsTech professional development intranet page. The procedure outlines that managers are responsible for ensuring all new employees receive a full induction and training program and for monitoring new employees' progress throughout induction.

Until April 2018, TAFE Queensland did not require new employees complete the information privacy training module at induction. When it identified that the completion rate was low (10%), it resolved to make information privacy training mandatory for all new starters at induction. TAFE Queensland also plans to make information privacy a mandatory component of its 2018-19 refresher training program for all existing staff.

Information security

Two agencies, the Public Trustee and the department, require their employees to complete a mandatory information security awareness training module at induction. New staff at the Public Trustee have 20 days to complete the module and the department's new employees have 30 days.

The Public Trustee includes information security in the mandatory compliance program its employees must undertake each year. The department does not require its existing staff to revisit information security training periodically throughout their employment.

TAFE Queensland has taken some steps to mitigate information security risks. In October 2017, it trained approximately 2,000 employees about email security, in particular phishing and fraudulent URLs. TAFE Queensland is developing an information security awareness module and plans to roll it out as it consolidates into a single agency. It is too early to assess the effectiveness of this module in mitigating information security risks. TAFE Queensland has not mandated that all existing staff revisit information security training periodically.

Other awareness and education activities

The three agencies adopt similar approaches to raise awareness about information privacy and information security and remind staff of their obligations. These awareness activities include:

- logon splash screen and screen saver messaging about password protection, use of information and communication technologies and unauthorised disclosure of information

- communications to all staff reminding employees of their privacy obligations about unauthorised access to client information or promoting the role of the agency's information privacy officer
- online posts or articles in publications promoting and encouraging staff participation in Privacy Awareness Week.

The Public Trustee publishes its Information Privacy Plan on the website. The plan applies to all permanent full-time and part-time employees and all temporary employees. It guides employees in applying the information privacy principles in their roles.

The Public Trustee did not require new employees to read and acknowledge the plan as part of their induction. During this audit, the Public Trustee included a link to the Information Privacy Plan in the training module and recommended new employees read the plan.

The department has established a Privacy Contact Officer network. The network includes representatives from across the department. Its purpose is to communicate privacy messages to the department's different business units. The representatives give privacy advice to employees within their business unit. The network also serves to bring privacy issues to the attention of the department's Privacy Contact Officer in the Right to Information, Information Privacy Screening Branch. Meetings of the department's Privacy Contact Officer network cover topics like:

- reviewing forms collecting personal information
- managing privacy breaches and privacy complaints
- reviewing privacy training statistics
- raising privacy issues arising since the previous meeting.

The network has not convened in 2018 due to recent, significant changes in structure, resources, reporting arrangements, systems and roles resulting from the transition to the NDIS and machinery of government changes. The department advised that it was not appropriate or timely to re-establish the network until those matters were finalised. We encourage the department to bring back the network to support communication, awareness and education about information privacy across the organisation.

TAFE Queensland has developed, and makes available to its staff, policies covering aspects of information security. These include an Information Management procedure and an Information Communication and Technology procedure. Both procedures apply to all TAFE Queensland employees. The induction procedure does not refer to them. There is no training about them and no process to ascertain whether TAFE Queensland has made its employees aware of these two procedures.

TAFE Queensland has drafted an Information Security policy, an Acceptable Use policy and a Privacy of Personal Information guideline. The draft policies and guideline outline the agency's commitment to mitigating information risks. TAFE Queensland intends to implement them as it continues to consolidate into a single agency. It is too early to assess their effectiveness in raising staff awareness and mitigating privacy and information security risks.

Confidentiality provisions in the agency's enabling legislation

All staff are bound to a declaration of secrecy under section 15 of *The Public Trustee Act 1978*. They sign the declaration when commencing with the agency thus acknowledging that they will not divulge information to any person except where authorised by law, such as under chapter 3 of the *Information Privacy Act 2009*.

The Public Trustee has an established process to ensure staff are aware of, and have understood, their obligations under its enabling legislation. This increases staff awareness and reduces the risks of privacy breaches resulting from unauthorised disclosure.

The department and TAFE Queensland also have duty of confidentiality provisions in their respective enabling legislation. Section 92 of the *Community Services Act 2007* and section 66 of the *TAFE Queensland Act 2013* prescribe each agency's obligations. These sections provide that staff cannot disclose agency information, including personal information of clients, except in specific circumstances. However, the department and TAFE Queensland cannot effectively demonstrate that they ensure their staff are aware of, and understand, the confidentiality obligations specific to their enabling legislation.

Recommendations

We recommend that the Department of Communities, Disability Services and Seniors:

1. within six months, mandates periodic refresher training on information privacy and information security for all employees.

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*.

We recommend that TAFE Queensland:

3. within six months, implements its decision to mandate training on information privacy for all new employees.

4. within six months, makes training about information security mandatory for all new employees.

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*.

6. within six months, mandates periodic refresher training on information privacy and information security for all employees.

7. within twelve months, finalises, implements and educates all employees about its:
   - Information Security policy
   - Acceptable Use policy
   - Privacy of Personal Information guideline.

We also recommend that all agencies subject to the *Information Privacy Act 2009*:

a. include information privacy and information security training in their **mandatory induction process** for all employees.

b. **mandate periodic refresher training** on information privacy and information security for all employees.

4 Training material

For training to be effective, it must be comprehensive, accurate and relevant to the context of the agency. Practical scenarios and revision questions should relate to the employee's functions and demonstrate how to apply information privacy and security when undertaking their day-to-day duties. Agencies can adopt tailored training packages specific to their work, or supplement general information privacy and security training with agency specific training.

We expect that the 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.

Conclusion

The three agencies have adopted information privacy training modules that are accurate and consistent with the *Information Privacy Act 2009*. The content of the information privacy training for TAFE Queensland gives a robust overview of this Act and the privacy principles, and is sufficient for employees to understand their obligations and to mitigate privacy risks adequately. The Public Trustee and department's information privacy modules were less comprehensive.

The Public Trustee amended its information privacy training module during the audit to include additional content. It also proposes to supplement the module with relevant sections of its Information Privacy Plan. This approach will be more effective in raising employee awareness of all privacy obligations and mitigating privacy risk.

The department's information privacy module provides a good overview for employees to understand their obligations under the Act. The inclusion of more practical scenarios will make it more effective as a tool for mitigating privacy risks.

The information security training of the Public Trustee and the department is comprehensive. The modules meet the agencies' needs in raising staff awareness of potential security threats to information assets. They are an effective tool for mitigating information security risks.

The lack of comprehensive information security training at TAFE Queensland means that it cannot be sure its staff are familiar with all their information security obligations. TAFE Queensland proposes to incorporate relevant components of information security from its policies and procedures into its information security awareness training. This approach will increase TAFE Queensland's ability to mitigate information security risks.

Information privacy

Each agency has an information privacy training module that is self-paced and time efficient for their employees to complete. The modules include a series of revision questions to test the employee's understanding. The employee must pass these revision questions to complete the training.

The Public Trustee and the department have information privacy training modules with solid and accurate content. They cover most of the elements we would expect to see in the training material.

The Public Trustee's information privacy module gives a good overview of the *Information Privacy Act 2009* and the privacy principles. It has material about the use of closed circuit television cameras. It also includes useful slides reminding staff that inappropriate access to, and disclosure of; information is a breach of the Code of Conduct. These slides are particularly good at reinforcing the expected behaviours of employees handling personal information.

During the audit, the Public Trustee amended its information privacy module and included slides about transferring information outside Australia, binding contractors and privacy officer contact details. It proposes to supplement the training module with sections of its Information Privacy Plan about collecting personal information and storing and securing personal information.

The department's information privacy module gives a good overview of the Act and the privacy principles. It includes most of the elements we expect to find, including transferring personal information outside Australia and binding contractors. The slides on Information Privacy Principle 4 are particularly good in reinforcing the types of physical and operational controls employees can use to protect personal information when carrying out their duties.

However, the module does not include enough agency specific scenarios or revision activities that illustrate in a practical way how the Act and the privacy principles apply in an employee's day-to-day role.

TAFE Queensland bases its information privacy training module on the resource we make available to agencies. The module is accurate and gives a robust overview of the Act and the privacy principles. It includes all the topics we expect to see in a comprehensive information privacy training, such as:

- explaining what privacy is and how it differs from confidentiality
- applying the privacy principles
- explaining exemptions to the privacy principles
- dealing with privacy complaints
- binding contracted service providers
- transferring personal information outside Australia.

TAFE Queensland tailors the scenarios in its module to illustrate how the Act and privacy principles apply in practice.

Information privacy training – TAFE Queensland

Activity: Applying IPP2

"*Tony rings his local TAFE campus to find out about an upcoming event. Tony agrees to be added to a mailing list about the event and provides his name and address. After completing the call, the Customer Service Officer finds Tony's file on another database and copies the information across, including information about Tony's ethnic origin and religion.*

Could this be a breach of the IP Act? Click on the correct option to continue."

Activity: Applying the use and disclosure principles

An 18 year old student is undertaking apprenticeship training with TAFE Queensland.

A parent turns up at the TAFE's customer service counter accompanied by a police officer. The parent tells the Customer Service Officer that she and her daughter – the apprentice - had a big fight about a week ago and the she hasn't heard from her daughter since.

The parent says that she just wants to make sure that her daughter hasn't done anything 'stupid' – like move to a new city. The parent says she has asked the police to attend with her just in case her daughter has 'got herself in any trouble'.

The police officer says that while there are no real concerns about the daughter's safety at this stage, it would assist everyone if this could be confirmed through the daughter's attendance at her course over the last week. The Customer Services Officer advises that the student has been in attendance for this time.

Has the Customer Services Officer breached the student's privacy? Click on the correct option to continue.

Information security

The Public Trustee and the department have adopted information security training modules. The modules are self-paced and time efficient for their employees to complete. They include a series of revision questions to test the employee's understanding.

The Public Trustee's information security module is based on the eight CyberSense videos from the Australian Signals Directorate at the Department of Defence. The videos are about:

- dangers of allowing other persons to access work computers
- risks of conducting sensitive business on a mobile wireless network
- laptop security
- dangers of phishing and other email scams
- risks of accessing sensitive information from public terminals
- risks of using unauthorised devices or untrusted media from an unknown source
- dangers of socially engineered emails designed to download malicious software.

The final video is a recap of the course content.

The department's information security module also includes the eight CyberSense videos. It has additional content such as using Cisco Registered Envelope Service to secure emails and 10 ways to be safe when using mobile devices. The module contains links to relevant departmental policies and informs employees that the department considers inappropriate or unauthorised access to information as a breach of the Code of Conduct.

TAFE Queensland's current training on information security is missing key components of information security. It has a fraud awareness training module accessible on the intranet and runs various campaigns mostly targeted on phishing emails and fraudulent URLs.

TAFE Queensland has policies and procedures that cover elements of information security but they do not form part of a structured training module on information security. For example, the Information Communication and Technology procedure advises users of their responsibilities to protect, secure and support TAFE's facilities, devices, services and systems. It outlines unacceptable behaviours such as sharing information that may be confidential or private (including passwords) or using other email systems.

The draft Information Security policy and Acceptable Use policy, once approved and implemented, would supersede the procedures. They outline an employee's responsibility regarding information security and the acceptable use of information. They also include practical references such as use of devices and password security.

TAFE Queensland intends to implement them as it restructures into a single agency. It has developed a draft concept for an information security training module. It is too early to assess the effectiveness of the proposed policies and the concept for the training module is currently not detailed enough to form a view on its content.

Recommendations

We recommend that the Public Trustee:

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

We recommend that the Department of Communities, Disability Services and Seniors:

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

We recommend that TAFE Queensland:

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

We also recommend that all agencies subject to the *Information Privacy Act 2009*:

c. ensure the **training content** on information privacy and information security is comprehensive, contemporary and tailored to the agency's context.

5 Enrolment and monitoring systems and processes

Education and training reinforces an agency's privacy culture and reduces the likelihood and impact of privacy and information security risks.

For agencies to deliver training effectively, their enrolment and monitoring 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.

We examined whether the audited agencies have effective systems and processes to make sure all eligible employees complete the information privacy and information security modules.

Conclusion

The Public Trustee and the department have established processes for enrolling staff in, and monitoring completion of, the information privacy and information security training modules.

While the Public Trustee achieves a high completion rate, its current monitoring process does not support timely completion of training. Its new learning management system scheduled for implementation in 2019 should see more staff completing their training within the specified timeframe.

The training completion rates for the department indicate that its process for ensuring staff enrol and complete the relevant training modules is not always effective. This can adversely affect the department's ability to mitigate privacy and information security risks.

TAFE Queensland has not enabled, for the information privacy module, the monitoring function of its learning management system. The low training completion rate reflects the optional nature of employees choosing to enrol and complete the training on information privacy. This affects TAFE Queensland's ability to mitigate privacy and information security risks.

Detailed findings

Enrolling and monitoring training

The three agencies use a learning management system for delivering their training. They have different processes to enrol staff and monitor training completion.

The Public Trustee's Strategic Workforce Services team within the Human Resource branch is responsible for enrolling staff in information privacy and information security training, and for monitoring completion. Line managers are responsible for ensuring new staff complete their

training. The managers receive a quarterly report identifying new employees who have yet to complete the training.

For existing staff completing refresher training, the Strategic Workforce Services team generates a weekly email reminder from the learning management system. This reminder email goes directly to the employee but not to their line manager. The Public Trustee intends to rollout a new learning management system in 2019.

The department's Learning Management team enrols new employees into the online induction modules. The system sends an email to new employees informing them of their enrolment. It also sends reminder emails to employees who have not completed the module but not to their line manager or supervisor.

New employees, such as Residential Care Officers who do not necessarily have access to the department's information technology network, attend face-to-face training. The department records their attendance in the system.

The department has a devolved process for checking that staff complete the mandatory induction modules. While the Learning Management team is responsible for enrolling new staff into the relevant modules, course content owners such as the department's Information Privacy unit or the Information Services branch are responsible for following up on course completions. The course content owners report quarterly to the relevant departmental governance body on training completion.

TAFE Queensland does not have an established process to monitor whether employees complete the information privacy training module. Its learning management system is able to monitor training completion and TAFE Queensland has activated this functionality for other modules, for example workplace health and safety. It has not done so for the information privacy module.

Public Trustee – training completion rates

New employees at the Public Trustee must complete training modules on information privacy and information security at the start of their employment. Between 1 July 2016 and 31 December 2017, the Public Trustee enrolled 227 new starters in these modules. This consisted of 97 staff categorised with 'Employee' employment status and 130 as 'Temporary'.

Four out of five (80.2%) new employees completed the information privacy module. The completion rate for the information security module was slightly higher (87.7%). Temporary staff have a lower completion rate than 'Employees'.

Table 1: Training completion rates

	Completed	Not completed	Completion rate
Information privacy			
Employee	84	13	86.6%
Temporary	98	32	75.4%
Total	**182**	**45**	**80.2%**
Information security			
Employee	89	8	91.8%
Temporary	110	20	84.6%
Total	**199**	**28**	**87.7%**

At the time of our audit, new starters had three months to complete the information privacy module and 20 business days to complete information security. Most new starters who completed the training modules did it within the specified periods.

Table 2: Timeliness of new staff completing training

	Total completed	Completed within time	Not completed within time	Rate completed within time
Information privacy	182	164	18	90.1%
Information security	199	153	46	76.9%

Of the 18 new starters who did not complete the information privacy module within the prescribed period, one took 330 days to complete the module and another two employees were in excess of 200 days.

About three quarters of new starters who completed the information security module did it within the specified period. Of the 46 new starters who did not complete the module within the specified period, three took in excess of 200 days.

At the time of our audit, information privacy was not a core module that employees must revisit annually. While current employees can re-enrol in the module at any time, no employee had taken up this opportunity. From February 2019, the Public Trustee will require all existing staff to complete the training on information privacy annually, within 20 days.

The Public Trustee introduced its information security training module in September 2016. It enrolled 654 staff in the module between 30 September and 10 July 2018. In total, 611 existing

staff completed the module with a further 26 in-progress. There were 17 cancelled registrations, including 11 for staff who completed the training under another registration.

Existing staff must revisit the information security training annually. In October 2018, the Public Trustee rolled out its annual refresher training in information security. It expects all staff to complete the training by early November 2018.

Department of Communities, Disability Services and Seniors – training completion rates

The audit scope for the department excludes Disability Services employees directly affected by the transition to NDIS. It also excludes staff who have transitioned to the Department of Child Safety, Youth and Women as part of the machinery of government changes in December 2017. To keep within scope, we selected from the iLearn Enrolment report new starters in Accommodation Support and Respite Services and corporate functions. The findings that follow relate specifically to these services and functions.

Between 1 July 2016 and 31 December 2017, 445 new starters commenced with the department's functions subject to this audit. This consisted of 245 casuals, mostly in Accommodation Support and Respite Services, 179 full-time employees and 21 part-time staff.

The completion rate for new employees was 82.9% for information privacy and 80.7% for information security.

Table 3: Completion rates for information privacy and information security training

	Total	Completed	Not completed	Completion rate
Information privacy	445	369	76	82.9%
Information security	445	359	86	80.7%

The completion rate between new starters is not uniform. The vast majority (91.4%) of new starters within Accommodation Support and Respite Services completed the information privacy training compared to 60% in Corporate.

Similarly 88.9% of new starters in Accommodation Support and Respite Services completed the information security training compared to 41.3% in Corporate.

New starters have 30 days from the date of enrolment to complete the information privacy and information security modules. Two thirds of employees who completed both the information privacy and information security modules did so within the specified period. Sixteen new starters did not complete the information privacy or information security modules within the prescribed period; nine took in excess of 90 days with the longest being 588 days. Seven employees took between 31-90 days.

The department does not require all current employees to revisit information privacy or information security as part of a regular refresher-training program.

TAFE Queensland – training completion rates

Between 1 July 2016 and 31 December 2017, TAFE Queensland hired 1,722 new employees. Only 284 (16.5%) completed the online information privacy training, which is consistent with the module being optional for that period. TAFE Queensland mandated information privacy training in April 2018.

Table 4: Completion rates for information privacy training

	Total	Completed	Not completed	Completion rate
Information privacy	1,722	284	1,438	16.5%

At the time of our audit, TAFE Queensland did not require current employees to complete a formal refresher-training program on information privacy or information security. However, it runs periodic awareness activities to remind employees of their obligations. TAFE Queensland provided an email from SkillsTech to its staff in July 2018 about completing the online induction refresher and the information privacy training. However, these activities are informal and not universally applied to all staff.

Recommendations

We recommend that the Department of Communities, Disability Services and Seniors:

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.

We recommend that TAFE Queensland:

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

We also recommend that all agencies subject to the *Information Privacy Act 2009*:

d. implement systems and procedures to ensure all employees complete mandatory training on information privacy and information security when due.

Appendices

Appendix A – Agency responses

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

6 December 2018

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

Phone: 3213 9160
Officer: Josephine Giles
Email: governance@pt.qld.gov.au

AUDIT – AWARENESS OF PRIVACY OBLIGATIONS

Dear Ms Rangihaeata

Thank you for your letter, dated 21 November 2018, enclosing the draft report to Parliament on your recent audit of awareness of privacy obligations.

The Public Trustee provides a range of services to the Queensland community including financial management for those with impaired decision-making capacity, making Wills and Enduring Powers of Attorney, estate and trust administration services and legal services. We place a high value on informing our staff of their responsibility to maintain the confidentiality and security of the information we collect from our clients to deliver these services. This contributes to our clients and the Queensland community maintaining confidence and trust in our role.

It was encouraging to read the positive assessment in your report of our commitment to our obligations under the *Information Privacy Act 2009*. As noted in the report, we have already implemented some actions in response to the findings of the audit such as including our information privacy training module in mandatory annual training. Planned enhancements to our Learning Management System in 2019 will deliver improved follow-up mechanisms to ensure training is completed within required timeframes.

As outlined in the attached action plan, I agree with your recommendation to enhance our current training module with the suggested content and confirm the changes will be implemented within the agreed timeframes.

I would also like to pass on my sincere thanks to your staff for the assistance they provided throughout the conduct of the audit.

Should you require any further information, please do not hesitate to contact Ms Josephine Giles, Senior Director, Governance and Risk on (07) 3213 9160.

Yours sincerely

Peter Carne
The Public Trustee of Queensland

Encl/...

Agency response and action plan – Public Trustee

OIC recommends:-		**Agency response and any proposed management action**	**Nominated owner**	**Nominated completion date**
#	Recommendation			
8.	within three months, supplements its information privacy training with the contents of its Information Privacy Plan.	*Agreed – the Public Trustee will supplement our Information Privacy training module with content from the Information Privacy Plan which is relevant to the agency's functions and employee roles.*	*Josephine Giles, Senior Director, Governance & Risk*	*30 April 2019*

Queensland Government

Office of the
Director-General

Department of
Communities, Disability Services and Seniors

Our reference: COM 07896-2018

06 DEC 2018

Ms Rachael Rangihaeata
Information Commissioner
Rachael.Rangihaeata@oic.qld.gov.au

Dear Ms ~~Rangihaeata~~ Rachel

Thank you for your letter of 21 November 2018 regarding the completion of your audit into agencies' educating and training employees about their privacy and information security obligations.

I appreciate the opportunity to comment on the proposed report to Parliament including the recommendations made. After careful consideration, I have agreed with all four of the recommendations made and this is reflected in the attached *Agency response and action plan* which I have completed. I have no further comments to make on the report.

The professional approach in which your audit team conducted the audit in consultation with officers from the Department of Communities, Disability Services and Seniors (DCDSS) is also recognised and acknowledged.

If you require any further information or assistance in relation to this matter, please contact Mr Scott Findlay, Acting Chief Human Resources Officer, Human Resources and Ethical Standards, Corporate Services, DCDSS on 3224 8667.

Yours sincerely

Clare O'Connor
Director-General

Enc (1)

1 William Street
Brisbane Queensland 4000
GPO Box 806 Brisbane
Queensland 4001 Australia

Agency response and action plan – Department of Communities, Disability Services and Seniors

OIC recommends:-		**Agency response and any proposed management action**	**Nominated owner**	**Nominated completion date**
#	Recommendation			
1.	within six months, mandates periodic refresher training on information privacy and information security for all employees.	The Department of Communities, Disability Services and Seniors (DCDSS) agrees with the recommendation and will implement mandatory periodic refresher training on information privacy and information security for all employees.	Director, HR Services, Systems and Reporting	30 June 2019
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*.	DCDSS agrees with the recommendation and will establish a process that ensures new employees have read and understood at induction their duty of confidentiality under the *Communities Services Act 2007* (the Act). The Act has relevance to employees specifically undertaking duties relating to funding and contract management. DCDSS will consider broadening the scope of this recommendation to include other applicable legislation where confidentiality provisions are relevant to its employees e.g. *Disability Services Act 2006*.	Director, HR Services, Systems and Reporting	30 June 2019

OIC recommends:-		Agency response and any proposed management action	Nominated owner	Nominated completion date
#	Recommendation			
9.	within six months, complements its general information privacy training with practical examples and scenarios tailored to its context.	DCDSS agrees with the recommendation and will build on the existing examples that form part of the general information privacy training through the use of agency specific practical examples and scenarios.	Director, HR Services, Systems and Reporting	30 June 2019
11.	within six months, implement more robust systems and procedures to ensure all employees complete the mandatory training on information privacy and information security when due.	DCDSS agrees with the recommendation and will strengthen its systems and processes through enhancements to its reporting, using a centralised approach.	Director, HR Services, Systems and Reporting	30 June 2019

07 DEC 2018

Ms Rachael Rangihaeata
Information Commissioner
Level 7, 133 Mary Street
Brisbane Q 4000

Dear Ms Rangihaeata

Thank you for your letter dated 21 November 2018 regarding your audit on awareness of privacy obligations, and your subsequent meetings with my officers.

As stated in your report, TAFE Queensland has only recently merged into a single registered training organisation that brings together 12 institutes, across six regions, into one agency. Through this process TAFE Queensland has been consolidating its policies and procedures towards a single consistent approach. This consolidation has elements yet to be complete, which is evident in the findings of the report.

That said, TAFE Queensland maintains a commitment to high quality policies and procedures across the organisation and, in line with our role as a training organisation, we are also committed to high quality training for all of our staff.

Please find enclosed our agency response and action plan. TAFE Queensland is pleased to be able to agree to all the recommendations and advise that action has already been taken to either complete those recommendations or to ensure their completion in the near future.

If you require any follow up or clarification please contact Alan Chapman, Chief Information Officer at Alan.Chapman@tafeqld.edu.au or on (07) 3514 3764.

Thank you for your audit of our organisation. It has assisted TAFE Queensland to ensure that its practices in privacy and security are appropriate.

Yours sincerely

Mary Campbell
Chief Executive Officer
TAFE Queensland

Ref: TQ18/63395

A: Level 9, 133 Mary Street
Brisbane Queensland 4000
P: PO Box 16100
City East Queensland 4002
W: tafeqld.edu.au
ABN 72 898 805 093

Agency response and action plan – TAFE Queensland

OIC recommends:-		**Agency response and any proposed management action**	**Nominated owner**	**Nominated completion date**
#	Recommendation			
3.	within six months, implements its decision to mandate training on information privacy for all new employees.	Completed. Training on information privacy is included in induction to all new employees.	Alan Chapman Chief Information Officer, TAFE Queensland Phone: 07 3514 3764	Completed.
4.	within six months, makes training about information security mandatory for all new employees.	Completed. Training about information security is included in induction to all new employees.	Alan Chapman Chief Information Officer, TAFE Queensland Phone: 07 3514 3764	Completed.
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.*	Completed. A process to train new employees on published policies, procedures and guidelines on information privacy, information security and confidentiality obligations under the TAFE Queensland Act exists.	Alan Chapman Chief Information Officer, TAFE Queensland Phone: 07 3514 3764	Completed.
6.	within six months, mandates periodic refresher training on information privacy and information security for all employees.	Completed. Mandated refresher training on information privacy and information security will be provided to all employees annually, during January / February each year, commencing in 2019.	Alan Chapman Chief Information Officer, TAFE Queensland Phone: 07 3514 3764	Completed.
7.	within twelve months, finalises, implements and educates all employees about its: • Information Security Policy • Acceptable Use policy • Privacy of Personal Information guideline	On track for completion. Information Security and Acceptable Use policies have been implemented and education has been included in new employee induction and mandated refresher training. New Administrative Access Procedure and Privacy of Personal information Guideline is on track for publication by March 19 with awareness activities scheduled to occur during annual Privacy Awareness Week activities.	Alan Chapman Chief Information Officer, TAFE Queensland Phone: 07 3514 3764	31 March 2019

10.	within twelve months, incorporates relevant components of information security from its policies and procedures into its information security awareness training	On track for completion. Relevant components of information security are being added to new employee induction and mandated refresher training and will be in place for annual refresher in January / February 2019.	Alan Chapman Chief Information Officer, TAFE Queensland Phone: 07 3514 3764	18 January 2019
12.	within twelve months, implements systems and procedures to ensure all employees complete the mandatory training on information privacy and information security when due.	Completed. Procedure to ensure completion of induction and annual training exists. All mandatory induction and refresher training will be delivered through the organisation's Learning Management System which has been configured with automatic reminders and reports that will facilitate completion monitoring and reporting.	Alan Chapman Chief Information Officer, TAFE Queensland Phone: 07 3514 3764	Completed.

Appendix B – Methodology

We thank the staff of the audited agencies for their support and cooperation.

Mandate

We conducted this audit under section 135 of the *Information Privacy Act 2009*. The findings of the audit will inform our privacy awareness materials and strategies. Section 135(1)(b)(iv) of the *Information Privacy Act 2009* describes our training and education function.

We applied our Assurance Engagement Methodology[11] based on the standards set by the Australian Auditing and Assurance Standards Board.

Audit objective

The objective of the audit was to determine whether agencies educate and train their employees about their obligations under the *Information Privacy Act 2009* appropriately.

The audit assessed whether:

- agencies' education and training material covers information privacy adequately
- agencies educate and train their employees about information privacy.

In this audit, 'employees' means permanent, temporary and casual employees, whether employed full-time or part-time.

We used the following criteria:

Lines of inquiry	Criteria
1. The agency's education and training material covers information privacy adequately.	1.1 The agency has determined the privacy risks of its various functions. 1.2 The agency has identified that educating and training its employees about information privacy can mitigate the privacy risks. 1.3 The agency has adopted education and training processes and materials about information privacy that meet its need and are tailored to the risks.
2. The agency educates and trains its employees about information privacy.	2.1 Employees go through an induction process that covers information privacy at the start of their employment with the agency. 2.2 Employees receive education and training that covers information privacy at regular intervals or when necessary.

[11] Available on our website www.oic.qld.gov.au

Audit scope

The audit examined three government agencies that employ permanent, temporary and casual staff:

- The Public Trustee
- Department of Communities, Disability Services and Seniors
- TAFE Queensland

The audit did not examine the education and training content that does not relate to information privacy or confidentiality. The audit did not examine the education and training the agencies give to other types of employees or contingent workforce (volunteers, contractors, consultants, or others).

Audit process

The audit team worked with agency officers dealing with training and education, human resources, risk assessments and privacy. It gathered sufficient, appropriate evidence through:

- document review, including internal policies and procedures, staffing and training records
- system walkthrough
- interviews with relevant staff, management, external service providers and independent external consultants.