Office of the Information Commissioner
Queensland

Mitigating the risks of privacy breach through staff education

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

Report No. 1 to the Queensland Legislative Assembly for 2022-23

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 +61 7 3234 7373 or Freecall 1800 OIC QLD (1800 642 753)

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

ISBN: 978-0-6456316-0-9

November 2022

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 the findings of the Office of the Information Commissioner's audit – Mitigating the risks of privacy breach through staff education: How three government agencies educate and train their employees about their privacy and information security 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 the audited 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

Summary

The inadvertent or deliberate disclosure of personal information can have serious consequences for the individual whose privacy was breached, the agency storing the information 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*.

Since completing this audit Australia has seen one of the largest corporate data breaches when the personal information of millions of Australians was breached as a result of a cyberattack on Optus' network.

The impact of this breach has reverberated across the nation. It left many Australians pondering - *How secure is my personal information when I hand it over to an organisation?* All public sector agencies need to take heed of this as a reminder of the devastating impact a breach can have on the people affected and the reputation of the agency involved.

One of the key frontline safeguards agencies can implement to protect personal information is to ensure their employees understand their responsibilities and obligations when it comes to protecting the personal information of Queenslanders.

In December 2018, we tabled our report[1] on how three government agencies educated and trained their employees about their information privacy and information security obligations. We also made four recommendations to all agencies.

Training and education activities should be mandatory, 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 the training when due.

The need for educating and training employees in their obligations was reinforced by the Crime and Corruption Commission (CCC). In February 2020, the CCC released its report on Operation Impala which examined improper access to and dissemination of confidential information by public sector employees.

The CCC reported that education and awareness programs are critically important to achieve an effective information privacy culture. A clear understanding and awareness of information privacy requirements is therefore critical for mitigating risk and promoting compliance.

[1] Awareness of privacy obligations available at https://www.oic.qld.gov.au

This audit follows up on our 2018 recommendations to all agencies. The objective is to determine whether agencies educate and train their employees about their obligations under the *Information Privacy Act 2009* appropriately.

We examined the practices in place in three government agencies - the Department of Transport and Main Roads (DTMR), WorkCover Queensland and the Queensland Rural and Industry Development Authority (QRIDA).

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 the training in reducing privacy risk varies. For example, they have set different requirements for completing the training, adopted different training content, and established different processes to make sure employees complete the training.

They all have made training compulsory for new employees, but only DTMR and WorkCover Queensland mandate refresher training at regular intervals during employment with the agency.

It is encouraging to note that QRIDA had identified the need for its existing staff to undertake refresher training. However, at the time of the audit, it was still rolling out a new online learning management system that would deliver this training.

When existing staff do not complete periodical refresher training on information privacy and security they may forget or misunderstand their obligations over time.

The three agencies have adopted information security training content that is comprehensive and raise staff awareness of potential security threats to information assets. The content of their information privacy training is accurate and consistent with the Act, although QRIDA’s training is too high level to ensure staff understand all their privacy obligations in the context of their roles.

DTMR and WorkCover Queensland have established processes for enrolling employees in, and monitoring completion of, the information privacy and information security training modules at induction and for regular refresher training.

While DTMR achieves a high completion rate for employees undertaking refresher training, it is not always timely.

WorkCover Queensland achieves a high and timely completion rate for employees undertaking annual refresher training. However, its current monitoring process for completion of induction training is not working as effectively as it could.

QRIDA has a structured induction program which includes privacy and information security training. However, the way QRIDA was delivering information security training to new starters for the period under review had significant weaknesses. For example, it did not test new employees' understanding of their obligations but relied on their self-reporting. This means QRIDA cannot be sure that its staff understand what is expected of them to keep information safe.

While DTMR and Workcover Queensland have substantially implemented our 2018 recommendations, QRIDA has work to do to improve how it delivers education and training to raise employee awareness of their obligations and strengthen its privacy culture.

The transition to a new online learning management system is an opportunity for QRIDA to develop comprehensive training content that is tailored to its functions and needs. The agency also has the chance to incorporate knowledge assessments and strong monitoring and reporting processes that ensure employees complete mandatory training when due. The new system can help QRIDA better mitigate information privacy and security risks. We will examine the new system and associated training content and processes when we follow up the implementation of our recommendations.

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 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.

Mandatory training

The three agencies use education and training as a risk mitigation strategy. In two agencies, training on information privacy and information security at induction and at regular intervals during employment was mandatory for the period audited, 1 July 2020 to 31 December 2021. This is in line with our 2018 recommendations.

Figure 1 outlines the training requirements in the three audited agencies.

Figure 1

Training requirements

	DTMR	WorkCover Queensland	QRIDA
Information privacy training mandatory at induction	Yes	Yes	Yes – but limited in scope
Information security training mandatory at induction	Yes	Yes	Yes - but limited in scope
Information privacy training mandatory periodical refresher	Yes – annually	Yes - annually	Identified but not yet determined frequency of training
Information security training mandatory periodical refresher	Yes – annually	Yes - annually	Identified but not yet determined frequency of training

Source: Office of the Information Commissioner

At the time of our audit, QRIDA had recognised the need to run training programs more efficiently. It started rolling out a new online learning management system in early 2022. The agency advised that it intends to make refresher training in information privacy and security mandatory but did not indicate the frequency.

Training material

To be effective as a risk mitigation strategy, the training content must be contemporary, 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.

DTMR's information privacy module is robust and comprehensive. It appropriately informs employees of their obligations under the Act. The department uses video presentations within the module to illustrate in a practical way how the Act and the privacy principles apply in an employee's day-to-day role.

DTMR's Cyber Security Essentials module is interactive and informative. It raises employee awareness of the types of security threats and risks to the department's information and the types of measures employees can take to protect it.

All WorkCover Queensland employees must complete an online privacy module. While the content is accurate and gives a good overview of the Act, it does not cover all aspects of the privacy principles.

WorkCover Queensland has also developed a role specific, in-person presentation for new Customer Advisor and Claims Representative officers. This is a good approach that targets the privacy risk of a specific function.

WorkCover Queensland recognised the information security risks of remote working. It developed a training module supporting its Contemporary Mobile Workforce policy, which sets out the arrangements and expectations for employees working remotely.

For the period under review (1 July 2020 to 30 June 2021), QRIDA's training gave employees limited information on their privacy obligations. Information privacy training forms part of a broader package of training slides. The material does not explain why privacy is important. For example, it does not draw attention on the significant impact a privacy breach can have on the individual whose privacy has been breached or on the employee who committed the breach. The training does not adequately cover all aspects of privacy to properly inform staff of their privacy obligations.

Another weakness is the lack of knowledge-based assessment when completing the training. This means there is a risk that new staff do not fully understand their information privacy obligations before gaining access to systems and documents containing personal information.

QRIDA's training material includes slides about protecting information and systems, and on cybersecurity. There are links to information security policies and to a recorded training session on cybersecurity.

The video sufficiently informs staff about information security threats and the importance of taking information security seriously. However, it is not mandatory to view the video. QRIDA advised that it takes it on trust employees have read and understood the content of the information security policies. It does not monitor if new staff have watched the video.

Enrolment systems and processes

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.

DTMR uses a learning management system for most of its employees' training. There are different processes to enrol employees and monitor training completion. Line managers are responsible for following up outstanding training. There is an escalation process for employees who fail to complete training.

However, the process for monitoring timely training completion of existing employees is not working as effectively as it could. More than a quarter of the DTMR employees sampled did not complete the refresher training on information privacy by the due date.

When DTMR launched a new Cyber Security Essentials course in June 2020, its Information Security Management Board set a due date for existing employees to complete the module within up to five months given it was a new mandatory requirement. The current timeframe for completing this refresher course has since reverted to 30 days, in line with the refresher course on privacy. This shorter period is more effective as a risk mitigation strategy.

WorkCover Queensland's system automatically assigns and enrols new employees into online training modules based on their position and role. In addition, new Customer Advisors and Claims Representatives receive in-classroom presentations in information privacy and information release as part of their on-boarding.

Between 50 to 60 percent of new staff complete the online module within time. This means that the process for monitoring training completion is not working as effectively as it could.

Current employees must take part in an annual refresher training program, including information privacy and security. They are enrolled into the courses in January and have until the end of March to complete the online modules. WorkCover Queensland achieves a high completion rate (90 percent or more) by the due date.

The way QRIDA delivers compliance obligations training to new employees means there was no meaningful data we could use to assess completion rates and their timeliness. QRIDA's processes are insufficient to satisfy itself that new employees have actually read the privacy and information security related material.

For the audit period under review, QRIDA did not require current employees to complete a formal refresher training program on information privacy or information security.

QRIDA has an opportunity to implement strong monitoring and reporting processes as it rolls out its new learning management system.

Recommendations

We recommend that:

Queensland Rural and Industry Development Authority

1. within six months, implements processes that mandate information privacy and information security training:

- at induction for all new employees
- **annual** refresher training for all employees.

3. within twelve months, develops comprehensive information privacy training content that:

- allows employees to fully understand their obligations and responsibilities under the *Information Privacy Act 2009* and relevant policies
- is tailored to the context of the agency and helps employees understand how the topic relates to their day-to-day duties
- deals with employees' unauthorised access to personal information as outlined in the Crime and Corruption Commission's report into Operation Impala
- assesses the employees' knowledge and understanding of the topic
- includes details of the agency's privacy officer/champion to assist employees with privacy matters.

4. within twelve months, rolls out training in information privacy for all employees.

5. within twelve months, develops comprehensive information security training content that:

- allows employees to fully understand the types of information security threats, obligations and responsibilities for safeguarding information in accordance with the *Information Privacy Act 2009* and the authority's relevant policies
- is tailored to the context of the agency and helps employees understand how the topics relate to their day-to-day duties
- assesses the employees' knowledge and understanding of the topic.

6. within twelve months, rolls out training on information security to all employees.

7. within six months, incorporates unauthorised access to personal information as outlined in the Crime and Corruption Commission's Operation Impala report into its information privacy or information security training module.

10. within twelve months, implements robust systems and procedures to ensure all new and existing employees complete the mandatory training on information privacy and information security when due.

WorkCover Queensland

2. within six months, includes more comprehensive content on all privacy principles in its information privacy module to assist employees in understanding all their obligations under the *Information Privacy Act 2009*.

9. within six months, implements more robust systems and procedures to ensure all new employees complete the mandatory training on information privacy and information security when due.

Department of Transport and Main Roads

8. within six months, implements more robust systems and procedures to ensure all employees complete the mandatory periodic refresher training on information privacy and information security when due.

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**.

1 Context

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* (Qld).

One risk mitigation strategy agencies can adopt is to train and educate their employees about information privacy and information security obligations and expectations. The *Notifiable Data Breaches Report: July-December 2021* published by the Office of the Australian Information Commissioner[2] shows that human error is the source of 41% of data breaches.

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.

In December 2018, we tabled our report on how three government agencies educated and trained their employees about their information privacy and information security obligations. We made four recommendations to all government agencies:

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

The need for educating and training employees in their obligations was reinforced by the Crime and Corruption Commission Queensland (CCC). In February 2020, the CCC released its report[3] on Operation Impala which examined improper access to and dissemination of confidential information by public sector employees.

[2] Available at www.oaic.gov.au
[3] Available at www.ccc.qld.gov.au

The CCC reported that education and awareness programs are critically important to achieve an effective information privacy culture. A clear understanding and awareness of information privacy requirements is therefore critical for promoting compliance. It recommended agencies ensure that training[4]:

1. is developed and provided to all public sector employees prior to gaining access to any database that contains confidential information
2. is developed and provided annually to all public sector employees who have access to confidential information
3. 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*. The language used in the training material should be consistent and include explanation of items numbered 1 to 5 outlined in Recommendation 3.1
4. comprises a combination of online, face-to-face and video modules
5. records of the content and participation by employees are kept
6. is assessed annually to determine levels of retention and understanding of the content of the respective Information Privacy policy and supporting training material.

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

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 and information security adequately
- agencies educate and train their employees about information privacy and information security.

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 of relevant entities, including technologies, programs, policies and procedures, to identify privacy related issues of a systemic nature generally*

[4] Recommendation 4.1 – Operation Impala: Report on misuse of confidential information in the Queensland public sector: February 2020 available at www.ccc.qld.gov.au

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.

The scope of the audit includes three government agencies that employ permanent, temporary and casual employees:

- the Department of Transport and Main Roads (DTMR)
- WorkCover Queensland
- the Queensland Rural and Industry Development Authority (QRIDA).

The audit did not examine the education and training content that does not relate to information privacy or security. 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).

Department of Transport and Main Roads

DTMR is responsible for planning, managing and delivering an integrated transport network across road, rail, air and sea for the state. It manages major road and transport infrastructure projects as well programs to promote and provide customer safety on the state's transport network (rail, road, etc).

DTMR also delivers a range of services such as:

- testing and issuing of driver licences
- inspecting and registering motor vehicles
- overseeing personalised transport industry (taxi, limousine etc)
- providing passenger transit for bus, train and ferry.

In 2020-21, the department reported that it:

- issued an average of 25,513 drivers' licences per week
- processed on average 188,018 registrations per week
- provided 3.35 million face-to-face services to customers across its Customer Service Centres
- had 17.5 million customer interactions.

In providing these services, DTMR collects and holds a large volume of personal information. For example, the Customer Services Branch collects personal information about:

- customer name, address, date of birth and marital status
- customer restrictions

- driver licence status and history
- suspensions, cancellations, disqualifications and demerit points
- disability parking permit information.

As of 30 June 2021, DTMR employed 7,382 FTE employees. The actual employee headcount is 9,460 (full time 72%, temporary 7% and casual 21%).

WorkCover Queensland

Established under the *Workers' Compensation and Rehabilitation Act 2003*, WorkCover Queensland is the main provider of workers' compensation insurance in Queensland. The priorities of the agency are to:

- issue and renew workers' compensation insurance policies to employers
- manage the insurance claims process
- facilitate safe return to work programs with relevant stakeholders
- give advice and assistance to employers and workers about workers' compensation insurance, claims and options for early return to work.

In delivering these services, WorkCover Queensland in 2020-21:

- responded to 312,318 customer service calls to its contact centre
- insured 170,723 employers
- assisted 65,408 injured workers
- received 2,903 new common law claims.[5]

The personal information WorkCover Queensland collects and holds about a client depends on the service it supplies. For example, the Customer Group handling claims may hold highly personal and sensitive information such as health records, medical reports and client financial information.

As of 30 June 2021, WorkCover Queensland employed 836 FTE.[6] This consisted of full-time and part-time employees. The largest component of the agency's workforce is within the Customer Group.

[5] WorkCover Queensland 2020-2021 Annual Report available at www.worksafe.qld.gov.au

[6] WorkCover Queensland 2020-2021 Annual Report available at www.worksafe.qld.gov.au

Queensland Rural and Industry Development Authority

QRIDA is a statutory authority established under the *Rural and Regional Adjustment Act 1994*. Its purpose is to foster productive and sustainable regions and rural communities through financial assistance programs.

It is responsible for delivering government financial assistance programs to primary producers, businesses and non-profit organisations. It delivers these services through a network of 11 Regional Area Managers located in offices across Queensland.

QRIDA also provides additional programs and services to local, state and territory governments across Australia and the Australian Federal Government.

QRIDA is a specialist administrator of government financial assistance programs including:

- low interest loans to support businesses to grow and develop
- grants and rebates programs such as farm management and drought preparedness grants, and rural economic development grants
- farm debt services and mediation where it gives assistance to primary producers experiencing financial difficulties
- disaster recovery where it administers low interest loans and grants programs for those affected by disasters including tropical cyclones, bush fires and floods.

In administering these programs, QRIDA collects and holds highly personal and sensitive information about a client. The type of personal information collected and held varies across programs and can include client financial information.

In 2020-21, QRIDA reported that it:

- assessed and approved 16,700 applications for government assistance
- approved 193 First Start and Sustainability Loans under the Primary Industry Productivity Enhancement Scheme
- managed the COVID-19 Jobs Support Loan portfolio across 6,928 businesses supporting 86,464 local jobs.[7]

As of 30 June 2021, the authority employed 149 FTE (87 permanent and 62 temporary).[8]

[7] Queensland Rural and Industry Development Authority Annual Report available at www.qrida.qld.gov.au
[8] Queensland Rural and Industry Development Authority Annual Report 2020-2021 pg:14 available at www.qrida.qld.gov.au https://www.qrida.qld.gov.au/annual-report

Report structure

The report is structured as follows:

Section	Contents
Chapter 1	discusses privacy and information security risks, audit objectives and scope and a general overview of the audited agencies
Chapter 2	examines whether the audited agencies have mandated education and training at induction and at regular intervals (refresher training) as a tool for mitigating privacy risks
Chapter 3	discusses the content of the training material
Chapter 4	analyses how effectively the audited agencies deliver information privacy and information security training to their employees
Appendix A	contains the responses received from the audited agencies
Appendix B	outlines the audit methodology

2 Education and training as a risk mitigation strategy

Introduction

An effective privacy and information security culture promotes strong ethics and sets standards of behaviour when managing personal information. Education and awareness activities are essential proactive steps agencies can take to shape the behaviour of employees.

In 2018, we reported that, to support good privacy and information security practices, agencies needed to promote privacy awareness through education and training. Incorporating privacy and information security into training programs at induction and at regular intervals during employment with the agency is key to:

- building and maintaining a good privacy and information security culture
- minimising information privacy and security risks.

In 2020, the Crime and Corruption Commission Queensland (CCC) reported that effective policy, education and awareness programs are critically important to achieve a solid privacy and information security culture within Queensland Government agencies. It recommended that agencies provide information privacy and information security training annually to all public sector employees who have access to confidential information and assess levels of retention and understanding of content.

The CCC reported that key components which create and maintain employee awareness of privacy and information security messaging include:

- communication by leadership
- log-on warnings, screensavers and posters
- toolbox talks, newsletters and de-identified case studies.[9]

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, only DTMR and WorkCover Queensland have consistently made training on

[9] Operation Impala: Report on misuse of confidential information in the Queensland public sector: February 2020, pg 71 available at www.ccc.qld.gov.au

information privacy and information security mandatory both at induction and at regular intervals during employment with the agency.

QRIDA has mandated privacy and information security training at induction. At the time of the audit, it had identified the need for existing staff to undertake refresher training but had not yet rolled it out or determined the regularity.

The lack of systematic periodical refresher training on information privacy and security for all existing staff means their awareness of their obligations could fade over time. It also means that QRIDA is not mitigating privacy risks as well as it could.

Results

The three audited agencies have adopted strategies to mitigate their privacy and information security risks. The strategies include formal education and training on information privacy and information security as well as informal activities to raise general awareness.

Mandatory training

DTMR and WorkCover Queensland have set mandatory training on information privacy and information security at induction for all new employees and as regular refresher training for all existing employees.

DTMR's learning management system lists Information Privacy and Cyber Security Essentials training modules as mandatory for all employees. New and existing staff have 30 days to complete the online modules. They must complete them every year for compliance re-certification.

Due to the nature of their work, not all department employees have access to online training, like school crossing supervisors or RoadTek employees. DTMR developed alternative ways to deliver training to these employees, for example through annual presentations. For the purpose of this audit, we focused on employees having access to personal information and required to complete the online training modules.

All new and existing WorkCover Queensland staff must complete mandatory training in information privacy and information security. The agency's Learning Library page in 'MyPlace' lists the 11 mandatory compliance modules. They include:

- Privacy 2021
- Technology Use 2021
- Contemporary mobile workforce 2022.

New employees must complete the training within two weeks of commencing with WorkCover Queensland. The agency enrols all existing employees into the 11 mandatory compliance modules in January each year. Existing employees have until end of March to complete the modules.

New and existing employees at WorkCover Queensland receive the same general privacy training. The agency also delivers one-off, specialised training on information privacy and information release to new employees commencing in the positions of Customer Advisor and Claims Representative as part of their on-boarding at induction.

QRIDA includes information privacy and information security training as part of its induction for new employees. The Human Resources team conducts in person induction, either face to face or via Microsoft Teams.[10] The induction involves a high level presentation on compliance obligations.

Human Resources also send each new staff member an induction email with the compliance obligations presentation attached. The presentation includes links to the authority's Access to Information Framework document and the YouTube video of the cybersecurity training information session.

For the period under review (1 July 2020 to 30 June 2021), QRIDA did not require existing staff to undertake refresher training on information privacy and information security. It has since resolved to make refresher training mandatory for all existing employees. However, QRIDA has not specified the frequency of refresher training.

We recommend that the Queensland Rural and Industry Development Authority:

1. within six months, implements processes that mandate information privacy and information security training:

   - at induction for all new employees
   - **annual** refresher training for all employees.

Other awareness and education activities

One mitigation strategy agencies can adopt to reinforce and remind their employees of their privacy and information security obligations is through general awareness activities outside of formalised training processes. To achieve an effective information privacy culture, public sector agencies should undertake regular information privacy awareness campaigns.

[10] During the recent Covid-19 pandemic, QRIDA moved its induction of new employees to Microsoft Teams. It also uses Teams for new employees in regional offices who are unable to attend head office.

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

- making various policy documents on information privacy and information security available to all staff
- sharing online posts or articles promoting and encouraging staff participation in Privacy Awareness Week and other privacy and cybersecurity campaigns
- conducting information security drills to test employee awareness and responses to phishing emails.

WorkCover Queensland promotes and raises staff general awareness about information privacy and information security through a variety of channels.

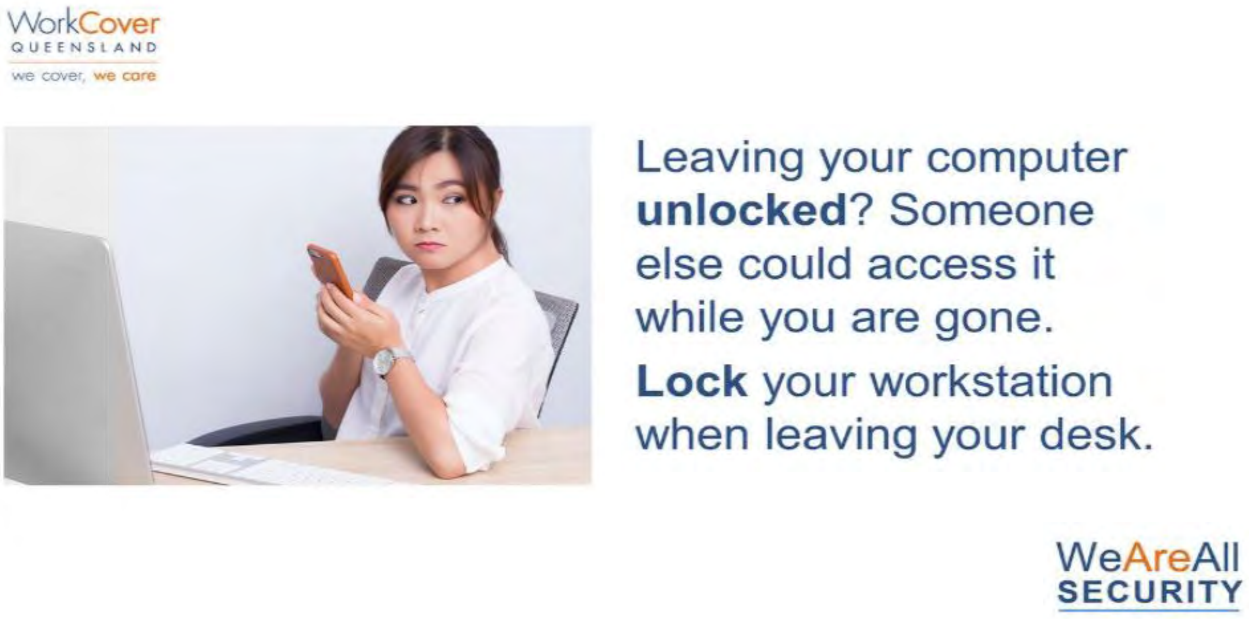
For example, it uses TV monitors positioned on walls throughout its office to raise employee awareness. The messages promote Privacy Awareness Week or remind employees to report suspicious emails and take other security measures including:

- protecting passwords
- securing and locking workstations whilst unattended.

WorkCover Queensland also promotes privacy awareness to all staff through rolling banners on its intranet homepage and through Yammer posts.

Figure 2A

Monitor slide on locking and securing unattended workstation



WorkCover
QUEENSLAND
we cover, we care

Leaving your computer **unlocked**? Someone else could access it while you are gone.

Lock your workstation when leaving your desk.

WeAreAll
SECURITY

Source: WorkCover Queensland

DTMR develops and releases annual information awareness campaigns to manage organisational risk and to inform and educate its employees who have access to one of the Queensland Government's largest information systems.

In 2021, the Customer Service Branch launched a campaign called ‘Protecting Information, Protects Everyone’.

The awareness campaign aimed to:

- highlight the responsibility of employees when accessing and using personal information
- reinforce the message for employees to act with diligence when accessing and using information
- provide an increased awareness of personal accountability that meets public expectations when handling personal information
- highlight the risks and consequences of accessing and leaking personal information.

To launch the campaign, Customer Service Branch employees depicted three real life de-identified scenarios. Through storytelling, they delivered key messages on the importance of protecting information:

- improving knowledge of risks and consequences of inappropriate access and use of personal information
- recognising impacts of inappropriate access and use to others through empathy
- where to refer suspected inappropriate access and use of information to.

All attendees agreed that the training was relevant, useful, and valuable and that they would recommend the training to others.

DTMR advised that as a result of the training, employees reviewed and questioned current business practices to ensure they comply with the legislation about accessing and disclosing personal information.

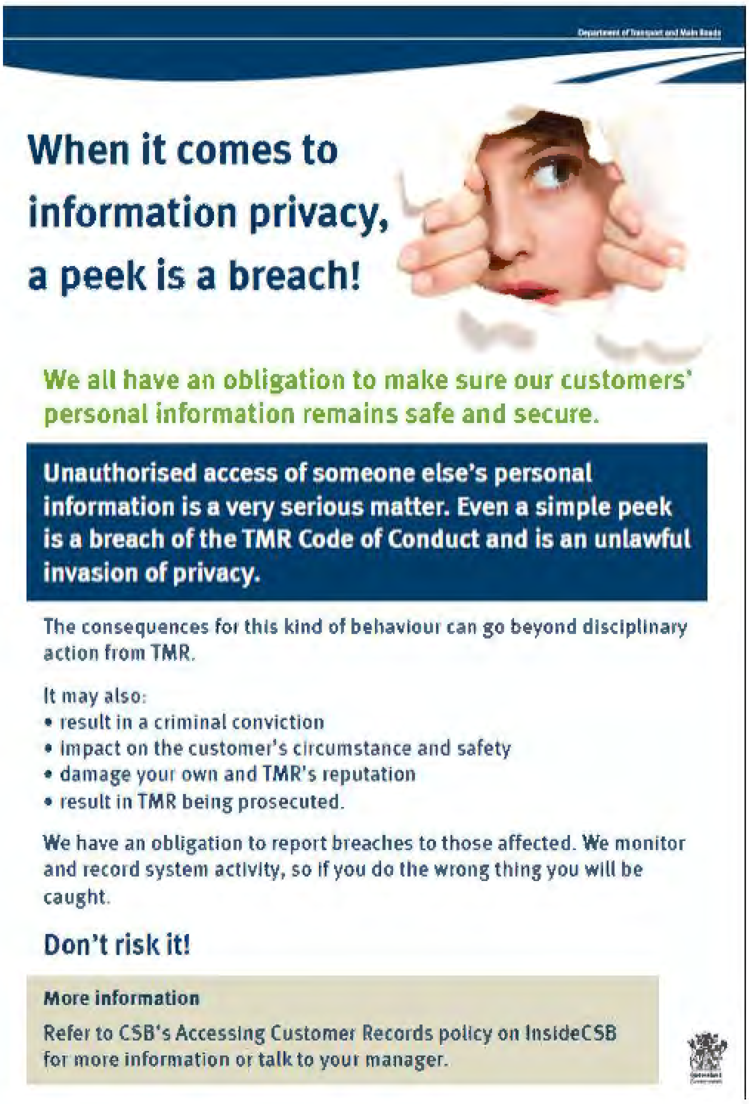
A component of the campaign included a short video highlighting the impacts and consequences to individuals when employees inappropriately access and disclose personal information.

DTMR now includes this video in its mandatory information privacy training module. The inaugural Privacy Champions meeting held during 2021 Privacy Awareness Week referred to the video as an effective way of addressing privacy risk.

DTMR has since shared this video with other government agencies, for example the Queensland Police Service, the Department of Education, the Department of Agriculture and Fisheries, the Department of Employment, Small Business and Training and TAFE Queensland.

Figure 2B

Campaign poster: Protecting Information Protects Everyone



Department of Transport and Main Roads

When it comes to information privacy, a peek is a breach!

We all have an obligation to make sure our customers' personal information remains safe and secure.

Unauthorised access of someone else's personal information is a very serious matter. Even a simple peek is a breach of the TMR Code of Conduct and is an unlawful invasion of privacy.

The consequences for this kind of behaviour can go beyond disciplinary action from TMR.

It may also:

- result in a criminal conviction
- impact on the customer's circumstance and safety
- damage your own and TMR's reputation
- result in TMR being prosecuted.

We have an obligation to report breaches to those affected. We monitor and record system activity, so if you do the wrong thing you will be caught.

Don't risk it!

More information

Refer to CSB's Accessing Customer Records policy on InsideCSB for more information or talk to your manager.

Source: Department of Transport and Main Roads

QRIDA has developed policies covering information privacy and information security. They are available to staff on its intranet.

The authority also raises staff awareness through participation in campaigns such as Privacy Awareness Week and Cybersecurity Awareness Month. It promotes these campaigns and reminds staff to be vigilant about protecting information of clients.

One good approach adopted by QRIDA is conducting one-off presentations to targeted staff when introducing new policies and procedures. This alerts staff to new standards of behaviour and gives the agency an opportunity to explain the practicalities and impact of the new policy.

For example:

- Client identification presentation to inform staff of the authority’s rollout of the new procedure, accompanying quick reference guide and updated forms for the new process.
- Privacy breach webinar to inform staff on how to respond to a privacy breach. The webinar includes information on mandatory reporting for certain malicious attacks and highlights some potential impacts a breach can have on the agency (reputation, financial costs) and the individual (physical/emotional harm, financial loss).

3 Training material

Introduction

In 2018, we found that 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 recommended all agencies ensure that information privacy and information security training material is comprehensive, contemporary and tailored to the agency's context. The training content should cover all relevant elements of information privacy and information security and be accurate and consistent with the Act and other resources.

The Crime and Corruption Commission reinforced the need for agencies to educate and train employees about their obligations in its 2020 report on Operation Impala.[11] It reported that education and awareness programs are critical to achieve an effective information privacy culture and promote compliance.

Conclusion

The three agencies have adopted information privacy training content that is accurate and consistent with the Act, but with varying level of detail.

DTMR's information privacy training is comprehensive and detailed. It appropriately informs employees of their obligations under the Act. WorkCover Queensland has tailored its training content to meet its needs. The modules are relevant in the context of an employee's role and functions. Minor improvements to the online course content would make the training more robust.

QRIDA's training material is high level and does not cover all aspects of privacy. This means it is less effective as a risk mitigation tool. There is a risk staff do not properly understand their privacy obligations.

The three agencies have comprehensive information security training. The modules raise staff awareness of potential security threats to information assets.

[11] Operation Impala - A report on misuse of confidential information in the Queensland public sector: February 2020 available at https://www.ccc.qld.gov.au/

However, the way QRIDA was delivering information security training to new starters for the period under review had significant weaknesses. It did not test new employees' understanding of their obligations but relied on their self-reporting.

The lack of knowledge testing at completion of the training means QRIDA cannot be sure that its staff understand what is expected of them to keep information safe.

The agency is transitioning to a new online learning management system. This is an opportunity for QRIDA to develop comprehensive training content that is tailored to its functions and needs. It also has the chance to incorporate knowledge assessments and monitoring processes. The new system can help QRIDA mitigate information privacy and security risks.

The three agencies address the possible consequences of unauthorised access to, and use of, personal information to varying degrees within their training. To be effective, the training should highlight the potential impacts unauthorised access can have on:

- the individual whose information was accessed
- the employee inappropriately accessing the information
- the agency.

Results

Information privacy

The online information privacy training modules for DTMR and WorkCover Queensland are self-paced and time efficient for new and existing employees to complete. They include a series of revision questions to test an employee's understanding. The employee must answer these questions correctly to complete the training.

The level of detail varies. DTMR's information privacy module is robust and appropriately informs employees of their obligations under the Act. It includes all the topics we expect to see in a comprehensive information privacy training module, such as:

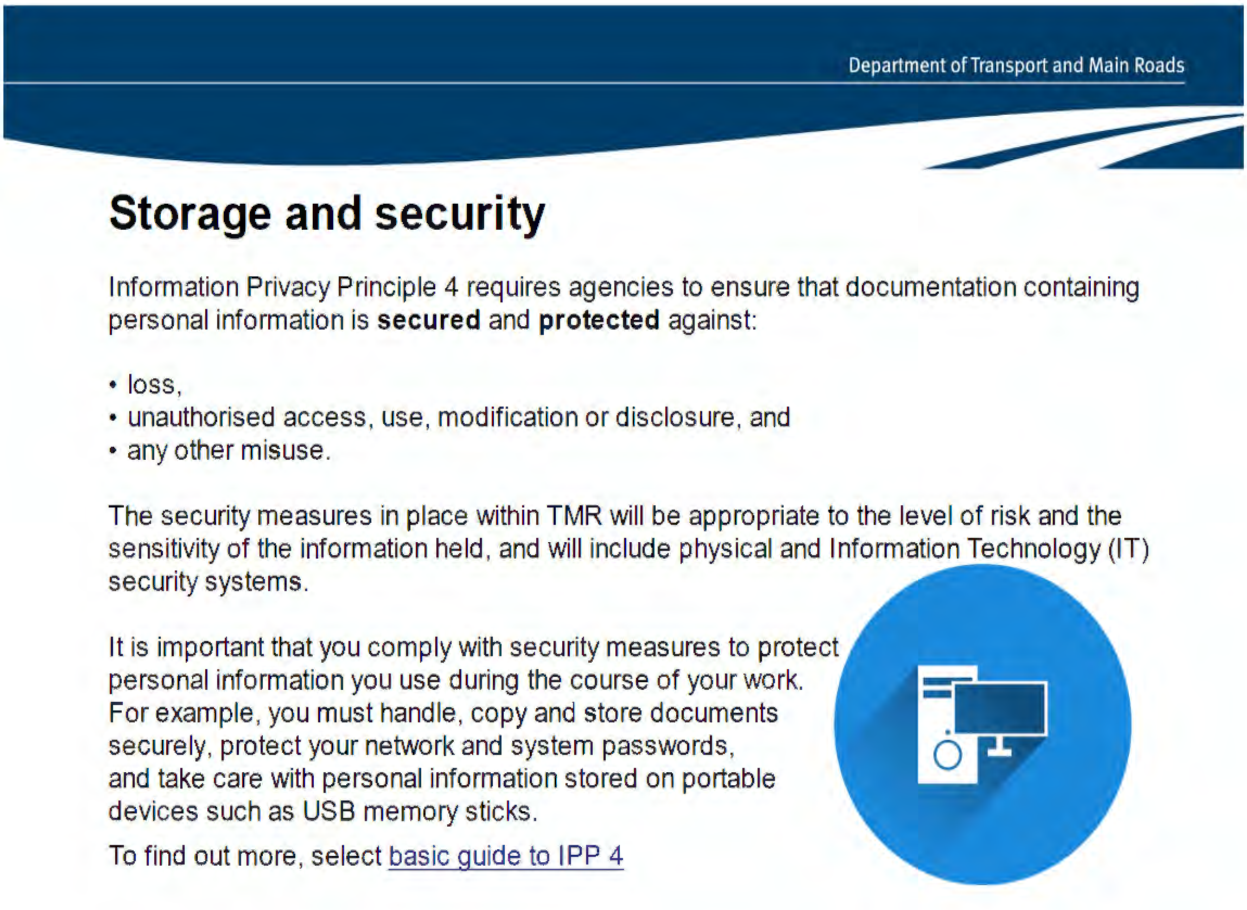
- what constitutes personal information
- the legislative basis for information privacy
- the information privacy principles including transferring personal information outside Australia and binding contracted service providers
- exceptions for other uses and disclosures of personal information
- privacy impact assessments
- unauthorised access to personal information (including the Criminal Code and Human Rights)
- privacy breaches and complaints.

DTMR uses video presentations within the module to illustrate in a practical way how the Act and the privacy principles apply in an employee’s day-to-day role.

The slides on ‘storage and security’ are particularly good in reinforcing the types of physical and operational controls employees can use to protect personal information when carrying out their duties.

Figure 3A

Storage and security slide from information privacy module



Department of Transport and Main Roads

Storage and security

Information Privacy Principle 4 requires agencies to ensure that documentation containing personal information is **secured** and **protected** against:

- loss,
- unauthorised access, use, modification or disclosure, and
- any other misuse.

The security measures in place within TMR will be appropriate to the level of risk and the sensitivity of the information held, and will include physical and Information Technology (IT) security systems.

It is important that you comply with security measures to protect personal information you use during the course of your work. For example, you must handle, copy and store documents securely, protect your network and system passwords, and take care with personal information stored on portable devices such as USB memory sticks.

To find out more, select basic guide to IPP 4

Source: Department of Transport and Main Roads

WorkCover Queensland has produced an online privacy module that all employees must complete at induction and as part of annual refresher training. It has also developed a tailored, in-person presentation new Customer Advisor and Claims Representative officers attend at induction. This presentation is not part of regular refresher training program. For the purpose of the audit, we focused on the online privacy training module all employees must complete.

The agency’s online privacy training module gives a good overview of the Act. It includes most of the elements we expect to see, such as:

- defining personal information
- outlining the information privacy principles

- information release provisions
- responding to privacy breaches.

Minor additions to the current content could make the module comprehensive and give employees a better understanding of how the *Information Privacy Act 2009* and privacy principles apply in their day-to-day activities. For example, section 33 about transferring personal information outside Australia and Chapter 2 Part 4 dealing with binding contracted service providers to the privacy principles.[12]

WorkCover Queensland uses a character named 'Captain Privacy' to better engage employees. The content about the privacy principles is very high level and does not always cover all aspects. For example, Captain Privacy's scenario for use and disclosure does not include how disclosure applies under Information Privacy Principle 11 (IPP 11).[13] A more detailed overview of each privacy principle supported by the Captain Privacy character scenarios could give practical examples of what this means in the context of the agency and the employees' day-to-day activities.

It would also be good for participants to know whom they can contact if they have questions about information privacy and their obligations.

During the audit, WorkCover Queensland advised that it was reviewing and amending its information privacy training module to address our findings. It intends to include more detailed explanation of the staff members' obligations under each privacy principle. It plans to roll out the training to new starters in 2022 and existing staff at the beginning of 2023.

We recommend that WorkCover Queensland:
2. within six months, includes more comprehensive content on all privacy principles in its information privacy module to assist employees in understanding all their obligations under the *Information Privacy Act 2009*.

For the period under review (1 July 2020 to 30 June 2021), QRIDA's training gave employees limited information on their privacy obligations. The information privacy training forms part of a broader package of training slides sent to all new staff and presented in person during the induction process. The slides are high level. They give an overview of the privacy principles but do not sufficiently cover all aspects of privacy to properly inform staff of their privacy obligations.

The slides do not include information about:

[12] The definition of privacy principles in schedule 5 of the IP Act makes the obligation to comply with section 33 and Chapter 2 Part 4 of the IP Act a privacy principle.

[13] IPP 11 sets out the exceptions allowing an agency to disclose personal information to a third party.

- obligations of staff for checking accuracy of personal information before using it (IPP8)
- an individual's right of access and amendment (IPP6 and IPP7)
- transferring personal information outside Australia and binding contracted service providers.

The slides also do not explain why privacy is important. For example, poor privacy practices can have significant impact on the individual whose privacy may be breached or on the employee who breached the individual's privacy. A privacy breach also affects public trust and the agency's reputation.

A significant weakness is that the training does not determine whether the participants understood how privacy applies to them in their day-to-day duties. There is no knowledge-based assessment that employees must pass to gain certification for successfully completing the training. This means there is a risk that new staff do not fully understand their information privacy obligations before gaining access to systems and documents containing personal information.

At the time of the audit, QRIDA is rolling out a new online learning management system to better deliver training across the agency. This is a great opportunity for QRIDA to ensure privacy training is comprehensive, contemporary and tailored to its needs. It is too early to form a view on the content of the proposed training module or assess its effectiveness as a strategy to mitigate privacy risks. This will be the subject of our follow-up audit.

We recommend that the Queensland Rural and Industry Development Authority:

3. within twelve months, develops comprehensive information privacy training content that:

- allows employees to fully understand their obligations and responsibilities under the *Information Privacy Act 2009* and relevant policies
- is tailored to the context of the agency and helps employees understand how the topic relates to their day-to-day duties
- deals with employees' unauthorised access to personal information as outlined in the Crime and Corruption Commission's report into Operation Impala
- assesses the employees' knowledge and understanding of the topic
- includes details of the agency's privacy officer/champion to assist employees with privacy matters.

We recommend that the Queensland Rural and Industry Development Authority:

4. within twelve months, rolls out training in information privacy for all employees.

Information security

Under IPP4 an agency must ensure that a document containing personal information is protected against, loss, unauthorised access, use, modification or disclosure. Protection must include security safeguards adequate to provide the level of protection expected.

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 unauthorised access, loss, misuse and disclosure.

DTMR and WorkCover Queensland 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.

DTMR's Cyber Security Essentials module is interactive and informative. It raises employee awareness of the types of security threats and risks to the department's information and the types of measures employees can take to protect it.

The module consists of two sections. Section 1 contains six modules that comprise video and knowledge quizzes. Section 2 is specific to DTMR. It includes information about:

- how to detect phishing emails and how to respond if the employee receives such an email
- departmental requirements for passwords
- maintaining security of department issued mobile devices
- use of department internet and email
- how physical security can protect against unauthorised access and includes examples of different security measures.

Participants must also read DTMR's Information security policy and Use of ICT Services, Facilities and Devices linked to in the module.

WorkCover Queensland has two training modules that address information security.

The Technology Use training module covers the topics of:

- access security is about passwords and password protection making WorkCover Queensland systems more secure
- cybersecurity software and cloud services discusses topics about cybersecurity (malicious software, phishing emails) and consequences to the agency such as breaches of privacy and unauthorised access to systems. It also covers topics on how to detect phishing emails

- accessing information and call recording offers tips for accessing information securely to ensure it remains confidential and only accessing information that the employee needs to undertake their job.

In 2017 WorkCover Queensland commenced a pilot exploring the opportunity for employees to work remotely. As its employees work with sensitive personal information, ensuring they were aware of and managed their privacy obligations when working remotely was a key component of the pilot.

Due to the success of the pilot, WorkCover Queensland rolled out the ability for employees to work remotely across the whole agency. It has developed a policy called Contemporary Mobile Workforce which sets out the arrangements and expectations for employees working remotely.

A training module supports the policy. WorkCover Queensland's People Operations team created the training module content in collaboration with the Privacy Committee to ensure it is both engaging and meeting the agency's obligations.

Case study

Contemporary mobile workforce – WorkCover Queensland

The training is delivered through WorkCover Queensland's online learning management system. It forms part of the mandatory suite of training modules that all employees must complete at induction and annually.

It includes a series of knowledge check questions to assess an employee's understanding of the agency's remote working arrangements and their obligations when working remotely.

There is a section on information privacy and information security which outlines what employees can do to maintain privacy and security while working remotely. For example:

- taking work calls and video meetings in private
- immediately notifying the office if work information, including personal information is lost, misplaced or stolen
- locking workstation screens when leaving the computer unattended.

The training supports WorkCover Queensland's Contemporary Mobile Workforce policy and helps to reinforce the agency's expectations of staff on what staff must do to ensure privacy and information security while working remotely.

QRIDA's training material includes slides about protecting information and systems and on cybersecurity. There is a link to the information security policies located on the intranet. QRIDA advised that it takes it on trust that employees read and understand the content of these policies.

In September 2019, all QRIDA staff attended a cybersecurity training information session. The agency recorded the session. The recording is included via a link to YouTube in the compliance obligations training package sent to all new starters at induction.

The video sufficiently informs staff about information security threats and the importance of taking information security seriously in light of IPP4 obligations. However, it is not mandatory to view the video. The authority does not monitor if new staff have watched the presentation.

Between September 2019 and May 2022, the video appears to have received 12 views. This indicates that the information security training presentation is not an effective tool for mitigating information security risks. QRIDA cannot be sure if its staff are familiar with all their information security obligations.

QRIDA advised that, as part of rolling out the new learning management system, it proposes to introduce a training module on information security. Again, this presents an opportunity for QRIDA to ensure that the module is comprehensive and tailored to the needs of the authority.

We recommend that the Queensland Rural and Industry Development Authority:

5. within twelve months, develops comprehensive information security training content that:

- allows employees to fully understand the types of information security threats, obligations and responsibilities for safeguarding information in accordance with the *Information Privacy Act 2009* and the authority’s relevant policies
- is tailored to the context of the agency and helps employees understand how the topics relate to their day-to-day duties
- assesses the employees’ knowledge and understanding of the topic.

We recommend that the Queensland Rural and Industry Development Authority:

6. within twelve months, rolls out training on information security to all employees.

Unauthorised access to personal information

In 2020 the Crime and Corruption Commission Queensland (CCC) examined the improper access and dissemination of confidential information by five public sector agencies. In its report on Operation Impala, the CCC identified that personal interest (accessing personal information out of curiosity or self-interest) was a driver for employees to misuse confidential information.

The CCC recommended that agencies increase training on the responsibilities involved when dealing with people's confidential information, and on the possible consequences of unauthorised access and use.

Each of the three agencies address this to varying degrees within their privacy and information security training modules.

Embedded within DTMR's privacy training is a short video ‘Protecting Information, Protects Everyone'. The video highlights the impact on individuals when employees inappropriately access personal information. It reinforces the message to employees that it is a crime to access personal information outside of the employee's official functions and includes the relevant sections of the Criminal Code to emphasise this.

WorkCover Queensland's training module includes a section on the code of conduct. This is a good example of how an organisation can outline its expectations on employees accessing personal information beyond their work needs. This section addresses the consequences of such actions to the employee, including disciplinary action or even a criminal offence. Although, to put context around why it is an unacceptable practice, it should also outline the consequences to the individual whose privacy has been breached. For example, potential serious harm, including to vulnerable members of our community such as victims of domestic and family violence.

QRIDA's cybersecurity training information video located on YouTube includes a section on ‘Information usage and information privacy'. It mentions that improper use and handling of personal information can affect the agency and its clients.

However the information about unauthorised access is not explicit enough. It should highlight the potential impacts unauthorised access can have on:

- the individual whose information was accessed (personal harm)
- the employee inappropriately accessing the information (disciplinary action, termination of employment or possible criminal action)
- the agency (damage to reputation, potential financial penalty).

We recommend that the Queensland Rural and Industry Development Authority:

7. within six months, incorporates unauthorised access to personal information as outlined in the Crime and Corruption Commission's Operation Impala report into its information privacy or information security training module.

4 Enrolment and monitoring systems and processes

Introduction

Education and training reinforce an agency’s privacy culture and reduce 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 systems and processes to make sure all eligible employees complete the information privacy and information security modules when due.

Conclusion

DTMR and WorkCover Queensland have established processes for enrolling staff in, and monitoring completion of, the information privacy and information security training modules at induction and for regular refresher training.

While DTMR achieves a high completion rate for employees undertaking refresher training, it is not always timely.

WorkCover Queensland achieves a high and timely completion rate for employees undertaking annual refresher training. However, its current process for monitoring completion of induction training is not working as effectively as it could.

When employees do not complete mandatory training when due, it weakens the effectiveness of training and education as a mitigation strategy for privacy and information security risks.

QRIDA has a structured induction program which includes privacy and information security training. However, its ability to determine whether new employees have read the training material is limited.

For the period under review, QRIDA did not require existing staff to undertake regular refresher training in information privacy and information security. The lack of such training means employees may forget or misunderstand their obligations over time. These weaknesses expose the authority to greater privacy and information security risks.

QRIDA has significant work to do to improve how it delivers education and training to raise employee awareness of their obligations and strengthen its privacy culture. It recognised this and, in early 2022, started to roll out of a new online learning management system. This is an opportunity to implement strong monitoring and reporting processes. We will examine the new system and associated processes when we follow up implementation of our recommendations.

Results

Department of Transport and Main Roads

DTMR uses a learning management system for most of its employees' training. There are different processes to enrol staff and monitor training completion.

When a new employee ID is created in the human resources system, it generates a profile in the learning management system. It also triggers automatic enrolment in the department's mandatory courses at induction.

The system assigns training modules based on the ID details and the new employee's branch/division. It sends an email to new employees about their enrolment. It also sends reminder emails to employees who have not completed a module.

The new employee's line manager is responsible for following up outstanding training. They have access to new employees' training status in the system. Managers also monitor training completion of new staff through the Induction Checklist sign-off process.

Existing employees are automatically enrolled into training one month before their certification is due to expire. They receive a notification that they have been enrolled into training and the due date for completion to maintain their compliance certification. Line managers are responsible for following up any outstanding training. There is an escalation process for employees who fail to complete the training.

DTMR reports divisional training statistics to the General Managers for their meeting with their Deputy Directors-General.

We analysed the training completion rates of new employees who commenced with DTMR's Customer Service, Governance and Human Resources branches between 1 July 2021 and 31 December 2021. These employees are the most likely to have access to personal information.

We did not examine the training records of new employees in other branches such as:

- RoadTek and school crossing supervisors who receive privacy training through different mechanisms as they do not have ongoing access to a computer
- employees who terminated employment between 1 July 2021 and 31 December 2021.

New employees must complete training on information privacy and information security within four weeks. For the period under review, DTMR enrolled 114 new starters in these modules. Most of them completed the training within the specified period.

Table 1: new staff training completion rates

	Total enrolled	Completed within time	Not completed within time	Rate completed within time
Information privacy	114	92	19	80.7%
Cyber Security Essentials	114	100	10	87.7%

Source: Office of the Information Commissioner

Note: the completion date for a small number of employees precedes their commencement date. DTMR explained this is because their employment status changed. We are not able to determine whether they completed the training within the specified period.

Of the 19 new starters who did not complete the information privacy module within the prescribed period, 9 completed it within one month of the due date, while 8 took between 91 and 177 days to complete the module.

The rate of completion for Cyber Security Essentials training was similar. The data indicates that 100 (87.7%) new starters completed the Cyber Security Essentials module within the specified period. Three employees completed it within a month of the due date.

Existing employees must complete the information privacy module every 12 months and have 30 days to do so.

DTMR enrolled 1,726 existing employees from the Customer Services, Governance, and Human Resources branches into the information privacy refresher training module.

Table 2: existing staff refresher training completion rates

	Total enrolled	Completed within time	Not completed within time	Rate completed within time
Information privacy	1,726	1,232	494	71.4%

Source: Office of the Information Commissioner

Nearly three quarters of employees completed the refresher training by the due date. Of the 494 employees who did not complete on time, 160 took 1-2 months, 249 took 2-6 months, 44 took 6-12 months and 41 had no completion date recorded.

This suggests that the process for monitoring timely training completion is not working as effectively as it could.

DTMR launched a new Cyber Security Essentials course in June 2020. While employees would generally have 30 days to complete a training module, the Information Security Management Board decided to set a due date of 30 November 2020 for staff enrolled between June 2020 and October 2020.

Because employees had up to five months to complete the module, DTMR was not mitigating its information security risk effectively as it could during this time, potentially exposing it to security threats.

DTMR enrolled 1,475 existing employees from the Customer Services, Governance and Human Resources branches into the Cyber Security Essentials module between June 2020 and October 2020. It enrolled a further 254 employees between November 2020 and December 2021.

Table 3: existing staff training completion rates

	Total enrolled	Completed within time	Not completed within time	Rate completed within time
Cyber Security Essentials (Jun 2020 to Oct 2020)	1,475	1,387	88	94.0%
Cyber Security Essentials (Nov 2020 to Dec 2021)	254	223	31	87.8%

Source: Office of the Information Commissioner

Note: Employees enrolled between June 2020 and October 2020 had a set due date of 30 November 2020 to complete the training. This reverted back to DTMR's mandated 30 days for all other employees enrolled into the module from November 2020.

A very high proportion of employees enrolled between June 2020 and October 2020 completed the module by the due date. DTMR advised that 56.9% or 839 staff completed the module within 30 days of being enrolled.

The completion rate dropped slightly to 87.8% for employees enrolled after this date. Of the 119 employees who did not complete on time, 56 took 1-3 months, 49 took 3-12 months and eight took longer than 12 months. A further six had no completion date recorded.

The current timeframe for completing the course on Cyber Security Essentials has reverted back to 30 days. This is in line with the timeframe for the privacy course. This shorter period is also more effective as a risk mitigation strategy.

We recommend that the Department of Transport and Main Roads:

8. within six months, implements more robust systems and procedures to ensure all employees complete the mandatory periodic refresher training on information privacy and information security when due.

WorkCover Queensland

WorkCover Queensland's system automatically assigns and enrols new employees into training modules based on their position and role. New employees receive an email advising them of the online training modules they must complete. It is the responsibility of the new starter's manager to ensure they are completing the allocated training. The Learning and Development team follows up directly with the new employee and their manager if the training is outstanding.

All new employees of WorkCover Queensland must complete 11 mandatory online compliance training modules within 14 days. Three modules relate to privacy:

- Privacy 2021
- Contemporary Mobile Workforce 2022
- Technology Use 2021.

In addition, new staff hired in the positions of Customer Advisor and Claims Representative receive in-classroom presentations in information privacy and information release as part of their on-boarding.

We examined the data for online training modules all new employees must complete. This excludes the in-classroom presentations.

Between 1 July 2020 and 30 June 2021, WorkCover Queensland hired 42 new employees.[14] Just over half completed the modules by the due date (within 14 days).

Table 4: new staff training completion rates

	Total enrolled	Completed within time	Not completed within time	Rate completed within time
Privacy 2021	42	25	17	59.5%
Technology Use 2021	42	22	20	52.4%
Contemporary Mobile Workforce 2022	42	21	21	50.0%

Source: Office of the Information Commissioner

[14] This figure does not include new employees who left WorkCover Queensland during the audit period.

This suggests that the process for monitoring whether new employees complete the mandatory online training on time is not working as effectively as it could.

The rate of completion within 28 days of being booked into the course is higher but not sufficient to ensure all new employees are fully aware of their privacy obligations:

- Privacy 2021 (76.2%)
- Technology Use 2021 (76.2%)
- Contemporary Mobile Workforce 2022 (66.7%)

No completion dates were recorded for four employees enrolled in the Privacy and Technology Use modules, and for one employee enrolled in the Contemporary Mobile Workforce module.

For the Contemporary Mobile Workforce 2022 course, 13 new employees took from 33 to 101 days to complete the course. WorkCover Queensland advises that as part of the completion process for the module, staff need to get their Contemporary Mobile Workforce agreement approved. This agreement includes other checks on technology and workplace health and safety.

We recommend that WorkCover Queensland:
9. within six months, implements more robust systems and procedures to ensure all new employees complete the mandatory training on information privacy and information security when due.

All WorkCover Queensland current employees must take part in an annual refresher training program. Existing staff are enrolled into the courses in January, including information privacy and information security. They have until the end of March to complete the online modules. The system sends a reminder email to employees before the training due date.

The Learning and Development team monitors completion of online training and notifies managers when training remains outstanding. WorkCover Queensland reports the progress of the annual compliance training to the Board. The update includes a summary of the percentage of learning activities completed.

WorkCover Queensland enrolled 876 existing staff into the online compliance modules in January 2021.[15] A very high proportion of employees completed the modules by the due date.

[15] This figure excludes 85 employees who ceased employment with WorkCover Queensland during 2020-21 and 38 employees on extended leave.

Table 5: existing staff training completion rates

	Total enrolled	Completed within time	Not completed within time	Rate completed within time
Privacy 2021	876	809	67	92.4%
Technology Use 2021	876	809	67	92.4%
Contemporary Mobile Workforce 2022	876	788	88	90.0%

Source: Office of the Information Commissioner

The high completion rates indicate that the process for ensuring staff enrol and complete training when due is effective.

Of the 67 employees who did not complete the Privacy 2021 and Technology Use 2021 training within time, respectively 32 and 35 did it within one month after the due date.

Queensland Rural and Industry Development Authority

QRIDA's Human Resources conduct new employee induction in two steps. It sends new employees an induction email with various attachments and links on compliance training. This includes slides on privacy and cybersecurity, and a link to YouTube video presentation. The email also specifies the due date for completion.

New starters must read the slides and the attachments. They use voting buttons to confirm they acknowledge and understand their compliance obligations. QRIDA manually tracks whether people have said they read the documents and Human Resources record the employees' responses in their respective files.

New employees also attend induction in person, or online if based in a region and unable to come to Head Office in Brisbane. As part of the in-person induction, a presenter goes through the compliance training material sent to the new employee in their induction email.

Watching the YouTube video on cybersecurity is optional. We note that between September 2019 and May 2022, the video training presentation seems to have received 12 views. The low viewing rate for the audited period reflects the optional nature of the training at the time.

Due to how QRIDA delivers compliance obligations training to new employees, there was no meaningful data we could use to assess whether new staff complete the training by the due date.

QRIDA's processes are insufficient to satisfy itself that new staff have actually read or viewed the privacy and information security related material. QRIDA advises that it takes it on trust that new employees read and understand the content of the training material and relevant policies.

For the audit period under review, QRIDA did not require current employees to complete a formal refresher training program on information privacy or information security.

In early 2022, QRIDA commenced rolling out a new learning management system that will help transitioning to an online platform. This means that QRIDA has a real opportunity to implement strong monitoring and reporting processes.

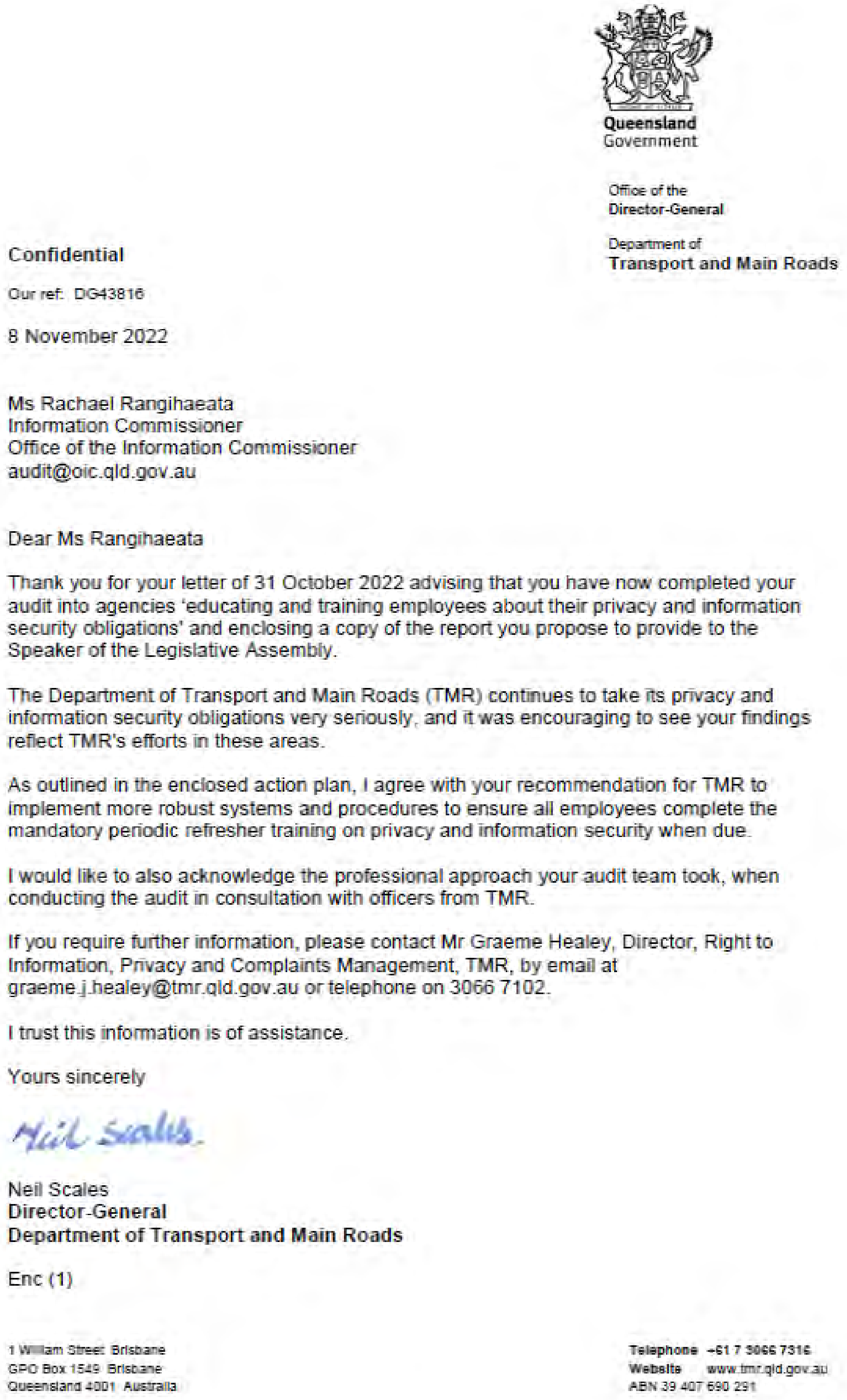
As the new system and associated processes for enrolling and monitoring training completion are not yet fully implemented, it is too early to assess their effectiveness. We will examine them in detail when we conduct the follow-up audit and also assess whether new and existing employees complete information privacy and information security training in a timely fashion.

We recommend that the Queensland Rural and Industry Development Authority:

10. within twelve months, implements robust systems and procedures to ensure all new and existing employees complete the mandatory training on information privacy and information security when due.

5 Appendices

Appendix A – Agency responses and action plan



Queensland
Government

Office of the
Director-General

Department of
Transport and Main Roads

Confidential

Our ref: DG43816

8 November 2022

Ms Rachael Rangihaeata
Information Commissioner
Office of the Information Commissioner
audit@oic.qld.gov.au

Dear Ms Rangihaeata

Thank you for your letter of 31 October 2022 advising that you have now completed your audit into agencies 'educating and training employees about their privacy and information security obligations' and enclosing a copy of the report you propose to provide to the Speaker of the Legislative Assembly.

The Department of Transport and Main Roads (TMR) continues to take its privacy and information security obligations very seriously, and it was encouraging to see your findings reflect TMR's efforts in these areas.

As outlined in the enclosed action plan, I agree with your recommendation for TMR to implement more robust systems and procedures to ensure all employees complete the mandatory periodic refresher training on privacy and information security when due.

I would like to also acknowledge the professional approach your audit team took, when conducting the audit in consultation with officers from TMR.

If you require further information, please contact Mr Graeme Healey, Director, Right to Information, Privacy and Complaints Management, TMR, by email at graeme.j.healey@tmr.qld.gov.au or telephone on 3066 7102.

I trust this information is of assistance.

Yours sincerely

Neil Scales

Neil Scales
Director-General
Department of Transport and Main Roads

Enc (1)

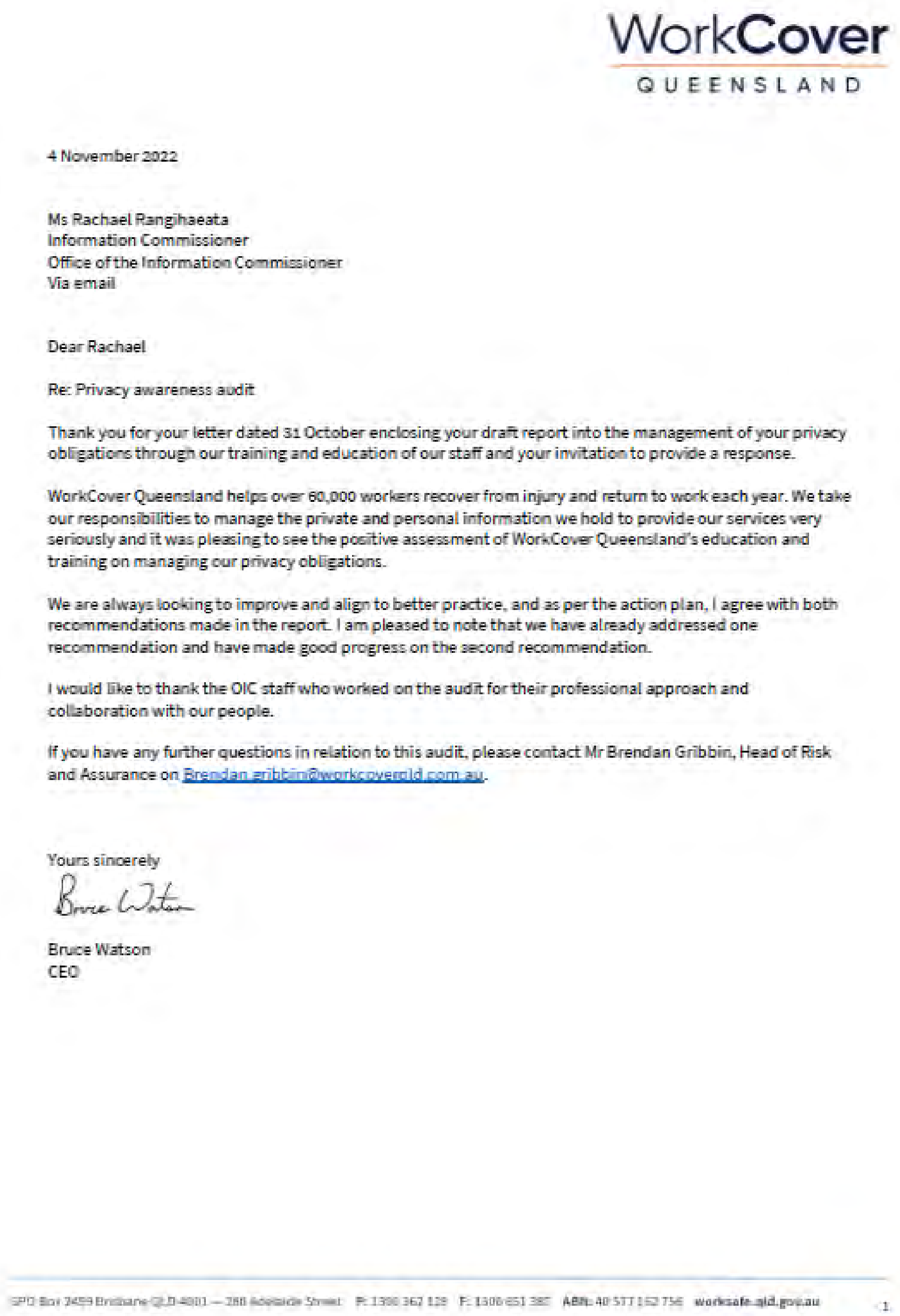
1 William Street Brisbane
GPO Box 1549 Brisbane
Queensland 4001 Australia

Telephone +61 7 3066 7316
Website www.tmr.qld.gov.au
ABN 39 407 690 291

Action Plan – Department of Transport and Main Roads

We recommended that the department:		Department of Transport and Main Roads response and proposed action		
No.	Recommendation	Agency response and proposed management plan	Nominated owner	Nominated completion date
8	Within six months, implements more robust systems and procedures to ensure all employees complete the mandatory periodic refresher training on information privacy and information security when due.	Recommendation accepted and on track for completion		
		Management actions: • Each month Human Resources Branch (through their existing Human Resources reporting suite) now provides TMR's Executive Leadership Team, for their awareness and action, details of mandatory training rates across TMR. • Human Resources Branch has implemented automated emails directed to managers, if one of their staff's training is overdue (either having never completed and falling outside of the one-month deadline, or failing to recertify by expiry date).	All General Managers, Executive Director, Directors and Managers.	31 March 2023

		Through the email reminders TMR has been promoting the use of the "My Teams" page in the Accelerate application to encourage managers to monitor all mandatory training completion for their employees. • At their branch leadership meetings, all General Managers (or equivalent) are expected to include, as an agenda item, the completion of mandatory training – to occur at least monthly.		
		• Via TMR's Information Privacy and Cyber Awareness communication campaigns, all employees and their mangers will be reminded of their obligations to complete the mandatory Information Privacy and Cyber Security Essentials courses. • Generate emails on a monthly basis to all General Managers listing their respective staff currently not certified in the Information Privacy or Cyber Security Essentials courses.	**Information Privacy** - Director RTI, Privacy and Complaints Management **Information Security** - Director Information Security, Risk & Governance	



WorkCover
QUEENSLAND

4 November 2022

Ms Rachael Rangihaeata
Information Commissioner
Office of the Information Commissioner
Via email

Dear Rachael

Re: Privacy awareness audit

Thank you for your letter dated 31 October enclosing your draft report into the management of your privacy obligations through our training and education of our staff and your invitation to provide a response.

WorkCover Queensland helps over 60,000 workers recover from injury and return to work each year. We take our responsibilities to manage the private and personal information we hold to provide our services very seriously and it was pleasing to see the positive assessment of WorkCover Queensland's education and training on managing our privacy obligations.

We are always looking to improve and align to better practice, and as per the action plan, I agree with both recommendations made in the report. I am pleased to note that we have already addressed one recommendation and have made good progress on the second recommendation.

I would like to thank the OIC staff who worked on the audit for their professional approach and collaboration with our people.

If you have any further questions in relation to this audit, please contact Mr Brendan Gribbin, Head of Risk and Assurance on Brendan.gribbin@workcoverqld.com.au.

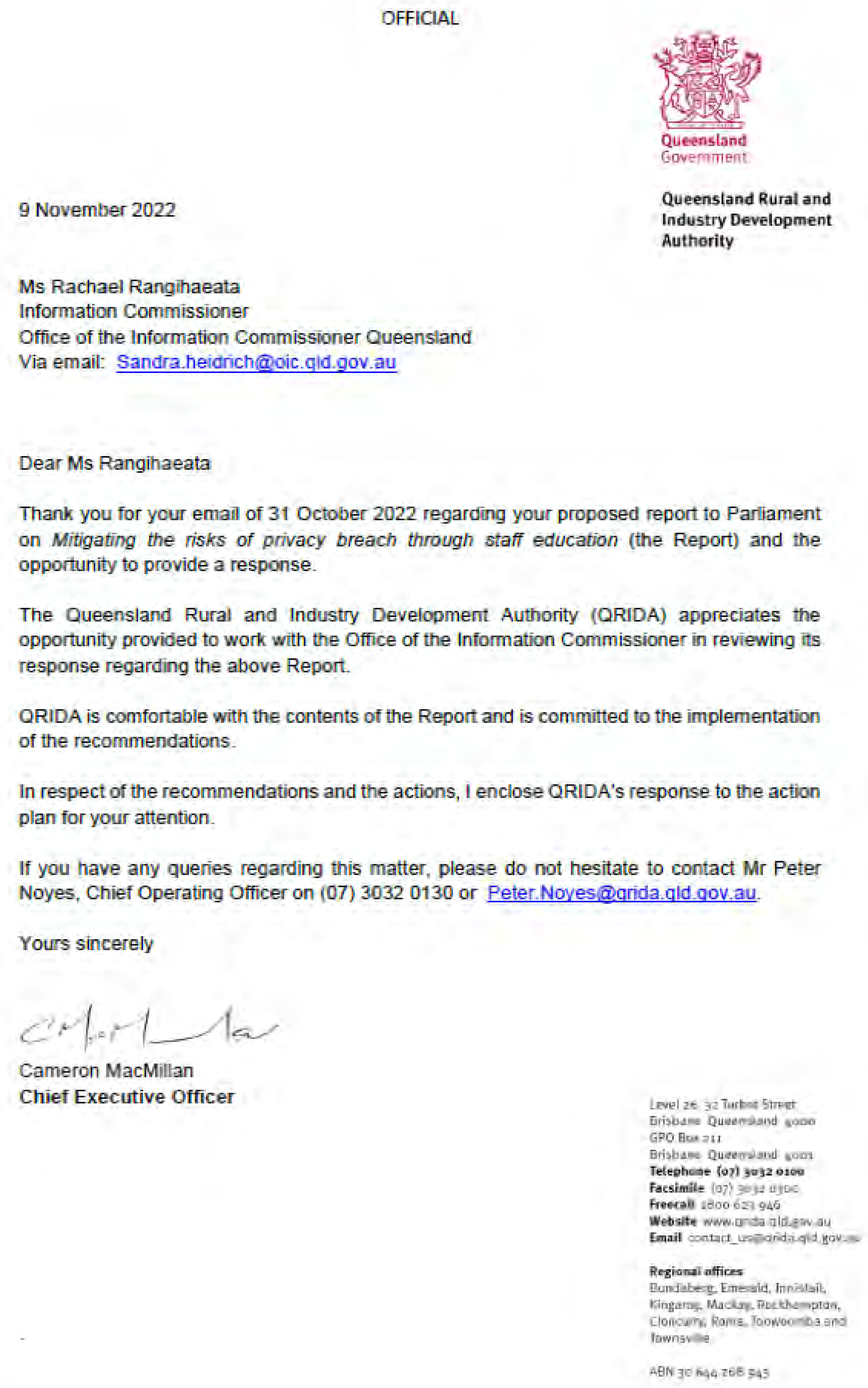
Yours sincerely

Bruce Watson

Bruce Watson
CEO

Action plan – WorkCover Queensland

We recommend the agency:		WorkCover Queensland response and proposed action
No.	Recommendation	
2	within six months, includes more comprehensive content on all privacy principles in its information privacy module to assist employees in understanding all their obligations under the *Information Privacy Act 2009*.	**Response**: Agree
		Proposed management action: The compliance modules will be updated to include the further information on obligations the OIC identified. This action has been completed.
		Nominated owner: Ms Trina Cash, Chair of WorkCover Queensland's Privacy Committee
		Nominated completion date: 30 November 2022
9	within six months, implements more robust systems and procedures to ensure all new employees complete the mandatory training on information privacy and information security when due.	**Response**: Agree
		Proposed management action: Reporting for any overdue compliance modules will be updated to weekly instead of the current monthly cadence from January 2023. This will allow more timely and regular follow up communication with people and their leaders for both the annual renewal for all employees and ongoing for any new employees. From January 2023 new employees will have 30 days to complete their compliance modules.
		Nominated owner: Ms Nadiene Van Gorp, Head of Learning and Development
		Nominated completion date: 31 March 2023



OFFICIAL

Queensland Government

Queensland Rural and Industry Development Authority

9 November 2022

Ms Rachael Rangihaeata
Information Commissioner
Office of the Information Commissioner Queensland
Via email: Sandra.heidrich@oic.qld.gov.au

Dear Ms Rangihaeata

Thank you for your email of 31 October 2022 regarding your proposed report to Parliament on *Mitigating the risks of privacy breach through staff education* (the Report) and the opportunity to provide a response.

The Queensland Rural and Industry Development Authority (QRIDA) appreciates the opportunity provided to work with the Office of the Information Commissioner in reviewing its response regarding the above Report.

QRIDA is comfortable with the contents of the Report and is committed to the implementation of the recommendations.

In respect of the recommendations and the actions, I enclose QRIDA's response to the action plan for your attention.

If you have any queries regarding this matter, please do not hesitate to contact Mr Peter Noyes, Chief Operating Officer on (07) 3032 0130 or Peter.Noyes@qrida.qld.gov.au.

Yours sincerely

Cameron MacMillan
Chief Executive Officer

Level 26, 32 Turbot Street
Brisbane Queensland 4000
GPO Box 211
Brisbane Queensland 4001
Telephone (07) 3032 0100
Facsimile (07) 3032 0300
Freecall 1800 623 946
Website www.qrida.qld.gov.au
Email contact_us@qrida.qld.gov.au

Regional offices
Bundaberg, Emerald, Innisfail, Kingaroy, Mackay, Rockhampton, Cloncurry, Roma, Toowoomba and Townsville

ABN 30 644 268 543

Action plan – Queensland Rural and Industry Development Authority

We recommend the agency:		Queensland Rural and Industry Development Authority response and proposed action
No.	Recommendation	
1	within six months, implements processes that mandate information privacy and information security training: • at induction for all new employees • **annual** refresher training for all employees.	**Response**: Accept
		Proposed management action: QRIDA undertakes to implement processes including establishing information privacy and information security training in our Learning Management System (LMS) for all new staff at orientation and annual revision training for all employees.
		Nominated owner: Executive Manager - Corporate Governance and Performance; and Senior Manager - Technology and Business Information
		Nominated completion date: May 2023
3	within twelve months, develops comprehensive information privacy training content that: • allows employees to fully understand their obligations and responsibilities under the *Information Privacy Act 2009* and relevant policies • is tailored to the context of the agency and helps employees understand how the topic relates to their day-to-day duties • deals with employees' unauthorised access to personal information as	**Response**: Accept
		Proposed management action: Establish comprehensive training in QRIDAs LMS for all employees. This training will include employees' obligations and responsibilities under the *Information Privacy Act 2009* and relevant policies and test knowledge and understanding of same. Establish protocols relating to unauthorised access to personal information and specific responsibilities under the dedicated privacy officer for QRIDA

We recommend the agency:		Queensland Rural and Industry Development Authority response and proposed action
No.	Recommendation	
	outlined in the Crime and Corruption Commission's report into Operation Impala - assesses the employee's knowledge and understanding of the topic - includes details of the agency's privacy officer/champion to assist employees with privacy matters.	**Nominated owner**: November 2023
		Nominated completion date: Executive Manager - Corporate Governance and Performance
4	within twelve months rolls out training in information privacy for all employees.	**Response**: Accept
		Proposed management action: Refine existing privacy training in QRIDAs LMS in accordance with finding of this review and make available to all employees
		Nominated owner: Executive Manager - Corporate Governance and Performance
		Nominated completion date: May 2023

We recommend the agency:		Queensland Rural and Industry Development Authority response and proposed action
No.	Recommendation	
5	within twelve months, develops comprehensive information security training content that: • allows employees to fully understand the types of information security threats, obligations and responsibilities for safeguarding information in accordance with the *Information Privacy Act 2009* and the authority's relevant policies • is tailored to the context of the agency and helps employees understand how the topics relate to their day-to-day duties • assesses the employee's knowledge and understanding of the topic.	**Response**: Accept
		Proposed management action: QRIDA undertakes to implement comprehensive information security training in our Learning Management System (LMS) for all new staff at orientation and annual revision training for all employees. Training to include security threats, obligations, and responsibilities for safeguarding information in accordance with the *Information Privacy Act 2009* and the authority's relevant policies. It will test knowledge and understanding of same.
		Nominated owner: Senior Manager - Technology and Business Information
		Nominated completion date: November 2023
6	within twelve months, rolls out training on information security to all employees.	**Response**: Accept
		Proposed management action: QRIDA undertakes to implement training on information security in our LMS for all employees.
		Nominated owner: Senior Manager - Technology and Business Information
		Nominated completion date: November 2023

We recommend the agency:		Queensland Rural and Industry Development Authority response and proposed action
No.	Recommendation	
7	within six months, incorporates unauthorised access to personal information as outlined in the Crime and Corruption Commission's Operation Impala report into its information privacy or information security training module.	**Response**: Accept
		Proposed management action: QRIDA undertakes to incorporate content related to unauthorised access to personal information as outlined in the Crime and Corruption Commission's Operation Impala report into its information privacy or information security training.
		Nominated owner: Executive Manager - Corporate Governance and Performance; and Senior Manager - Technology and Business Information
		Nominated completion date: May 2023
10	within twelve months implements robust systems and procedures to ensure all new and existing employees complete the mandatory training on information privacy and information security when due.	**Response**: Accept
		Proposed management action: QRIDA undertakes to implement robust systems and procedures with its LMS to ensure all new and existing employees complete the mandatory training on information privacy and information security when due.
		Nominated owner: Executive Manager - Corporate Governance and Performance
		Nominated completion date: November 2023

Appendix B – Methodology

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, 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* effectively.

Audit scope

The audit reviewed a small selection of government agencies, statutory bodies or departmental business units that employ permanent, temporary, and casual staff. The audit did not examine the education and training content that does not relate to information privacy and security or confidentiality. The audit did not examine the education and training the agencies provide to other types of employees or contingent workforce (labour hire, volunteers, contractors, consultants, or others).

We used the following criteria:

Lines of inquiry	Criteria
1. The agency's education and training material adequately covers information privacy and information security.	1.1 The agency has mandated information privacy and information security training at induction prior to new employees gaining access to systems and documents containing personal information. 1.2 The agency has mandated information privacy and information security refresher training for existing staff at regular intervals. 1.3 The agency raises general awareness about information privacy and information security through other channels (i.e. intranet postings, screensaver awareness messages, all staff awareness emails, etc).

Lines of inquiry	Criteria
	1.4 The agency has adopted education and training materials about information privacy and information security that meet its needs and are tailored to its operations and functions.
2. The agency educates and trains its employees about information privacy and information security appropriately.	2.1 The agency's employees complete information privacy and information security education and training at induction and at regular intervals. 2.2 The agency has adopted processes that ensure all employees complete the training when due. 2.3 The agency measures the effectiveness of its education, training and awareness activities.

Audit process

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

- document review, including internal policies and procedures, staffing, training content and training records
- system walkthrough
- interviews with relevant staff and management