Office of the Information Commissioner
Queensland

Follow-up of Report No. 1 for 2022-23

Mitigating the risks of privacy breach through staff education

Report No. 5 to the Queensland Legislative Assembly for 2024-25

Acknowledgement of Country

The Office of the Information Commissioner acknowledges Aboriginal and Torres Strait Islander peoples as the First Australians and recognises their culture, history, diversity and their deep connection to the land, waters and seas of Queensland and the Torres Strait.

We acknowledge the traditional custodians of the lands on which we operate and wish to pay our respects to their Elders past and present.

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 11, 53 Albert 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: 978-0-6489306-6-2

Office of the Information Commissioner
Queensland

June 2025

The Honourable Patrick Weir MP
Speaker of the Legislative Assembly
Parliament House
George Street
Brisbane QLD 4000

Tabling of Report No. 5 to the Queensland Legislative Assembly for 2024-25

Dear Speaker

I present for tabling a report prepared by the Office of the Information Commissioner (**OIC**) under section 135 of the *Information Privacy Act 2009* (Qld). It is a follow-up report and the third in a series that examined how agencies educate and train their employees about their obligations under the *Information Privacy Act 2009* (Qld).

'Follow-up of Report No. 1 for 2022-23

Mitigating the risks of privacy breach through staff education.'

In 2018-19, OIC audited three government agencies about their education and training practices. We found some weak elements and made four recommendations to all government agencies. These were designed to ensure agencies had effective training and were able monitor and check that their employees had complemented the training at the right time.

In 2022-23 we audited the Department of Transport and Main Roads (**Department**), WorkCover Queensland (**WorkCover**) and the Queensland Rural and Industry Development Authority (**QRIDA**) to ascertain whether that had embraced our four recommendations.

Results varied. Amongst areas of good practice, we found some weakness that was not effective at mitigating information privacy and information security risk. We made ten recommendations – seven to QRIDA, two to WorkCover and one to the Department, broadly:

- mandating education and training requirements
  Recommendation 1

- developing and rolling out comprehensive information privacy and information security training

  Recommendations 2-7
- implementing robust enrolment and monitoring systems to ensure information privacy and information security is completed when due

  Recommendations 8-10.

Each agency accepted our recommendations and proposed actions to implement them by November 2023.

In June 2024, OIC commenced a follow-up audit to assess each agency's progress in implementing the recommendations.

Our follow-up audit found progress. Five recommendations are fully implemented, four recommendations are partially implemented, and one recommendation has seen some progress made.

I respectfully request that you arrange for OIC's follow-up audit report to be tabled in the Legislative Assembly in accordance with section 193(5) of the *Information Privacy Act 2009* (Qld).

Yours sincerely

Joanne Kummrow

Information Commissioner

Table of contents

Summary

Background

The community expects government agencies to protect their personal information against loss, unauthorised access and other misuse as set out in the *Information Privacy Act 2009* (Qld) (**IP Act**).

Agencies can adopt various strategies to comply with their legislative obligations, minimise the risk of privacy breaches and meet community expectations. One strategy is to train and educate all their employees about information privacy and information security. To be effective and embed culturally within an agency, the training should be mandatory, regular and tailored. Systems and processes should also ensure all employees complete mandatory training when due.

In 2018-19, the Office of the Information Commissioner (**OIC**) examined how three government agencies[1] educated and trained their employees about their privacy obligations.[2] While each agency understood the value of education and training as a strategy to mitigate privacy risks, we found weak areas and improvement opportunities. We made four recommendations to all government agencies in the audit report tabled on 12 February 2019.

In 2022-23, we audited three other government agencies and examined how they educated and trained their employees about their privacy obligations. It followed on from the four recommendations we made to all government agencies in 2019.

We audited the Department of Transport and Main Roads (**Department**),[3] WorkCover Queensland (**WorkCover**) and the Queensland Rural and Industry Development Authority (**QRIDA**).

We found that the audited agencies were variously effective in adopting training and education as a risk mitigation strategy. There were areas of good practice but we also found significant gaps. We made ten recommendations in total – seven to QRIDA, two to WorkCover and one to the Department. Each agency accepted our recommendations. We tabled the audit report on 29 November 2022.

[1] The Public Trustee; the Department of Communities, Disability Services and Seniors; and TAFE Queensland.

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

[3] The audit examined three branches of the Department – Corporate Governance, Human Resources and Customer Service.

Follow-up results and conclusions

We started a follow-up audit in June 2024. The objective of the audit was to assess the implementation status of our 2022-23 recommendations.

We found that each agency made progress towards implementing our recommendations. **Figure 1** summarises the progress.

Figure 1

Implementation status of recommendations from 2021-22 audit

Agency	Status			
	Fully implemented	Partially implemented	Some progress	Total
Department		1		1
WorkCover	2			2
QRIDA	3	3	1	7
Total	5	4	1	10

Source: Office of the Information Commissioner

Of the ten recommendations made, six related to information privacy and information security training content and its rollout. QRIDA had the most work to do in this area to ensure that its training material was accurate, appropriate, tailored and deployed to its workforce.

We made one recommendation to each agency about ensuring that their employees complete the training when it is due. Each agency showed positive progress in particular fields. However, we did find pressing gaps in others.

Mandatory education and training

New and existing QRIDA employees must complete training in information privacy and information security. This is a marked improvement. The agency has also improved its induction and refresher training processes.

However, QRIDA does not spell out these obligations in policies or procedures that explicitly mandate the training.

Training content and rollout

The content of QRIDA's four relevant information privacy and security training modules is largely good, but does not meet the robust standards we expect.

There are many positive aspects that strengthen QRIDA employee’s understanding of information privacy and security. The inclusion of information about the potential impacts of unauthorised access to information is significant. Employees can access and use the modules easily – they are online and interactive.

Where QRIDA has tailored a training module content and assessment to its unique presence and function, its employees can link content to what they do day-to-day. However, this level of customisation is not consistent across the modules. Amending it would make for a more robust training vehicle.

The training has limited explicit connections to critical resources, such as the IP Act and the Information Privacy Principles. Together with unwarranted references to Commonwealth legislation, it generates a risk that QRIDA’s employees will not complete the training with adequate knowledge and skill in understanding their information privacy and information security obligations.

QRIDA has rolled out its training in information privacy and information security to its employees. This is a step forward to embed a positive culture that promotes compliance in information privacy and information security.

WorkCover updated its information privacy training. The high level approach we found in the initial audit has been replaced with more comprehensive, detailed and sophisticated content.

Enrolment and monitoring systems and processes

A crucial part of any training is ensuring that new and existing employees complete it within a reasonable and defined time.

Each agency made progress in ensuring that their employees complete information privacy and information security training. Only WorkCover was able to show us that its employees complete training and do so on time.

The Department has high training completion rates for the three branches we examined – over 96 percent. However, completion is not as timely.

QRIDA practices in this area have advanced since our 2022-23 audit. Its enrolment processes, learning management system and ability to collect details about completed training, form a good foundation. However, critical flaws in data capture, mean that the agency is unable to consistently demonstrate that training is completed when due.

Agency responses to the follow-up audit report

We provided a copy of this follow-up audit report to the Department, WorkCover and QRIDA for their review and invited them to provide a response.

The responses are in **Appendix A** to this report.

1 Context

The community trusts and expects that Queensland government agencies will handle their personal information appropriately, and safeguard it. The consequences of an inadvertent or deliberate disclosure of personal information can be serious – for the individual, the community, the agency concerned and its employees.

Agencies must protect personal information against loss, unauthorised access and other misuse as set out in the *Information Privacy Act 2009* (Qld) (**IP Act**). Effective compliance and strategies to support good practices can prevent and mitigate harm.

In 2023, the Office of the Australian Information Commissioner presented its report, *'2023 Australian Community Attitudes to Privacy Survey'*[4]. It identified community concerns about harm that may flow from a privacy breach.

> *Almost half (47%) of Australians said they had been informed by an organisation that their personal information was involved in a data breach in the 12 months prior to completing the survey in 2023.*
>
> *Three-quarters (76%) said they experienced harm as a direct result. Half (52%) saw an increase in scams and spam and almost a third (29%) said they had to replace key identity documents, such as a driver's licence or passport. One in ten (12%) experienced emotional or psychological harm.*[5]

The Australian Information Commissioner said, *'Australians see data breaches as the biggest privacy risk today, which is not surprising with almost half of those surveyed saying they were affected by a data breach in the prior year.'*[6]

We acknowledge these concerns and recognise the trust the Queensland community holds in agencies to handle their personal information appropriately. Reminding all agencies of the significant impact a privacy breach can have on the people affected and the reputation of the agency involved is not only important, but imperative to develop robust and effective practices. The Information Commissioner of Queensland has regulatory powers under the IP Act to look into systemic issues in relation to an agency's privacy practices.

[4] Available at https://www.oaic.gov.au/. Accessed 17 April 2025.
[5] Office of the Australian Information Commissioner, 'Australian Community Attitudes to Privacy Survey August 2023' at page 10. Available at https://www.oaic.gov.au/. Accessed 27 April 2025.
[6] Media release. Available at https://www.oaic.gov.au/news/media-centre/data-breaches-seen-as-number-one-privacy-concern-survey-shows.

Agencies can implement strategies to mitigate inadvertent or deliberate disclosure of personal information and prevent or mitigate harm. One measure is to train and educate agency employees about information privacy and information security obligations and expectations.

Government agencies that make employees aware of their privacy and information security obligations and expectations can better protect personal information against unauthorised access, loss, misuse and disclosure.

Training is only effective if it is robust. It should be regular, comprehensive, accurate and tailored to the context of each agency. Systems and processes must also be in place to ensure all employees complete mandatory training when it is due.

1.1 The agencies

We audited three government agencies – Department of Transport and Main Roads (**Department**),[7] WorkCover Queensland (**WorkCover**) and Queensland Rural and Industry Development Authority (**QRIDA**).

The Department is responsible for planning, managing and delivering an integrated transport network across road, rail, air and sea for the state.

At 30 June 2024, the Department had 11 860 employees.[8]

WorkCover is a statutory authority established under the *Workers' Compensation and Rehabilitation Act 2003* (Qld). Its functions include to provide insurance to businesses in Queensland who employ workers and encourage improved health and safety performance by employers.

At 30 June 2024, WorkCover had 1 095 employees.[9]

[7] The audit examined three branches of the Department – Corporate Governance, Human Resources and Customer Service.

[8] 8 536 full time employees, 1 257 part time employees, and 206 casual employees. Department of Transport and Main Roads Annual Report 2023–24 available at https://www.tmr.qld.gov.au/annualreport

[9] Excluding Directors, Contractors and Temporary Agency Staff WorkCover Queensland 2023-24 Annual Report available at https://www.worksafe.qld.gov.au/resources/publications/annual-reports/annual-report-2023-2024.

QRIDA is a statutory authority established under the *Rural and Regional Adjustment Act 1994* (Qld). It is a specialist administrator of government financial assistance programs including loans, grants and rebates.

At 30 June 2024, QRIDA had 215 employees.[10]

Further details about each agency appear at **Appendix B.**

1.2 The audits

The Information Commissioner conducts reviews, under section 135 of the IP Act, into personal information handling practices of agencies and, if appropriate, reports findings to the Speaker.

Our audits are critical to examine how agencies comply with their obligations under the IP Act and the *Right to Information Act 2009* (Qld). We conducted two earlier audits relevant to this follow-up.

2018-19 audit

In 2018-19, we examined how three government agencies[11] educated and trained their employees about their privacy obligations.[12]

We found that each agency recognised the value of educating and training their staff on information privacy and information security as a strategy to mitigate privacy risks. However, approaches and effectiveness varied. This generated weak elements. Agencies did not mitigate privacy risks as effectively as they could.

The audit report made specific findings and recommendations for improvement for the three agencies. It also made four recommendations to all government agencies, set out in **Figure 2**.

[10] Queensland Rural and Industry Development Authority Annual Report 2023-24 page:14 available at https://www.qrida.qld.gov.au/sites/default/files/2024-09/QRIDA_annual_report_23-24_Webcopy_PDF865KB.pdf

[11] The Public Trustee; the Department of Communities, Disability Services and Seniors; and TAFE Queensland.

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

Figure 2

2018-19 Recommendations to all agencies

No.	Recommendation
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.

Source: Office of the Information Commissioner

The audit report was tabled on 12 February 2019. It is published on our website.

2022-23 audit

This audit built on the four recommendations we made to all agencies in 2018-19 and incorporated some of the findings from the Crime and Corruption Commission's February 2020 report[13] on Operation Impala into misuse of confidential information by public sector employees.

In 2022-23, we audited three government agencies subject of this follow-up audit – the Department, WorkCover and QRIDA. We examined how these agencies educated and trained their employees about their obligations under the IP Act and focused on three key areas:

- education and training requirements
- training content
- enrolment and monitoring systems and processes.

The audit report was tabled on 29 November 2022. It is published on our website.

Key findings and conclusions

We found that the three agencies used education and training as a risk mitigation strategy with varying degrees of effectiveness.

[13] Available at www.ccc.qld.gov.au.

Figure 3 is from our 2022-23 audit. It outlines the **mandatory training requirements** in the three audited agencies at the time.

Figure 3

Mandatory training requirements

Timing	Topic	Department	WorkCover	QRIDA
At induction	Information privacy	Yes	Yes	Yes – but limited in scope
	Information security	Yes	Yes	Yes – but limited in scope
Periodical refresher	Information privacy	Yes – annually	Yes - annually	Identified but not yet determined frequency of training
	Information security	Yes – annually	Yes - annually	Identified but not yet determined frequency of training

Source: Office of the Information Commissioner

QRIDA recognised the need to run training programs more efficiently. It started rolling out a new online learning management system in early 2022 and told us that it intended to make refresher training in information privacy and security mandatory. It did not indicate the frequency.

We found each agency had marked differences in its **training material content**.

The Department's information privacy module was robust and comprehensive. Its Cyber Security Essentials module was interactive and informative. It raised employee awareness of the types of security threats and risks to the Department's information and the steps employees can take to protect it.

WorkCover's privacy training was accurate, but not comprehensive. It did not cover all aspects of the Information Privacy Principles. WorkCover recognised the information security risks of remote working, providing a training module supporting its Contemporary Mobile Workforce policy.

While QRIDA's training material did include information about protecting information and systems, it gave limited information on employees' privacy obligations. We also found a lack of knowledge-based assessment when completing the training. This meant there was a risk that new staff did not fully understand their information privacy obligations before gaining access to systems and documents holding personal information.

Each agency showed gaps in its **enrolment systems and processes*.***

The Department's processes for monitoring timely training completion of existing employees was not working as effectively as it could. For example, we found more than a quarter of Department employees sampled had not completed the refresher.

We found that between 50 to 60 percent of new WorkCover employees completed their privacy and information security training modules within time. This indicated the process for monitoring training completion for its new employees was not working as effectively as it could.

The way QRIDA delivered training to new employees meant there was no meaningful data we could use to assess completion rates and their timeliness. We found that QRIDA did not require current employees to complete a formal refresher training program on information privacy or information security.

Recommendations

We made ten recommendations to be implemented within six to twelve months after the audit report was tabled:

- **Recommendation 1:** QRIDA implements processes that mandate information privacy and information security training.
- **Recommendation 2**: WorkCover includes more comprehensive content on all privacy principles in its information privacy module.
- **Recommendation 3:** QRIDA develops comprehensive information privacy training content.
- **Recommendation 4:** QRIDA rolls out training in information privacy for all employees.
- **Recommendation 5:** QRIDA develops comprehensive information security training content.
- **Recommendation 6:** QRIDA rolls out training on information security to all employees.
- **Recommendation 7:** QRIDA 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.

- **Recommendation 8:** the Department 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 9:** WorkCover implements more robust systems and procedures to ensure all new employees complete the mandatory training on information privacy and information security when due.
- **Recommendation 10:** QRIDA implements robust systems and procedures to ensure all new and existing employees complete the mandatory training on information privacy and information security when due.

Each agency accepted our recommendations and proposed actions to implement them between November 2022 and November 2023.

1.3 2024-25 follow-up audit

In June 2024, we commenced a follow-up audit under section 135 of the IP Act.

The audit assesses whether the Department, WorkCover and QRIDA have implemented the ten recommendations we made in our 2022-23 audit about mitigating the risks of privacy breach through staff education.

Figure 4 explains the ratings we used in this report.

Figure 4

Implementation status ratings

Rating	Description
Fully implemented	The agency has implemented the recommendation substantially or in its entirety.
Partially implemented	The agency has implemented part(s) of the recommendation, but it has not fully satisfied the intent of the recommendation.
In progress	The agency has taken action to implement the recommendation and efforts to complete implementation are ongoing.
Some progress	The agency has taken preliminary steps to implement the recommendation. Progress is limited and the underlying issues are not yet addressed.

Source: Office of the Information Commissioner

Each agency reported its progress. QRIDA self-assessed its progress for implementation of Recommendation 7 as ‘In progress’. All other recommendations made to the three agencies were self-assessed as being ‘Fully implemented’.

NOTE: we used the legislative requirements in force at the time of our follow-up audit to assess the content of the training material. We acknowledge that these requirements will change when the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) commences.

Results

We reviewed the evidence received from each agency and performed risk-based checks to gain assurance on their self-reported actions and implementation status.

Each agency made progress in the three years since our 2021-22 audit report was tabled. **Figure 5** summarises the progress.

Figure 5
Implementation status of recommendations from 2021-22 audit

Rec	Agency	Fully implemented	Partially implemented	Some progress
Training requirements				
1	QRIDA		✓	
Training content and rollout				
2	WorkCover	✓		
3	QRIDA		✓	
4	QRIDA	✓		
5	QRIDA		✓	
6	QRIDA	✓		
7	QRIDA	✓		
Enrolment and monitoring systems and processes				
8	Department		✓	
9	WorkCover	✓		
10	QRIDA			✓
	TOTAL	**5**	**4**	**1**

Source: Office of the Information Commissioner

Chapters 2, 3 and 4 of this report present our findings on each agency's progress to implement the ten recommendations under the following headings:

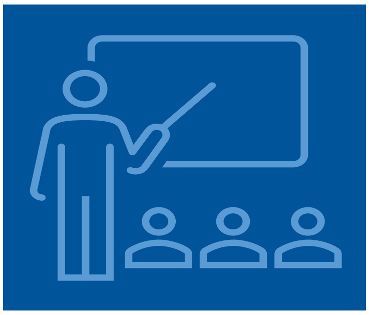
- Mandatory education and training – Recommendation 1
- Training material and rollout – Recommendations 2 - 7
- Enrolment and monitoring systems and processes – Recommendations 8 - 10.

2 Mandatory education and training (Recommendation 1)

2.1 Introduction

An effective privacy and information security culture is critical. It embeds strong ethics and sets standards of behaviour when managing personal information. It can also mitigate and minimise information privacy and information security risks. Education and awareness activities are fundamental to drive and shape the behaviour of employees. They are essential proactive steps agencies can take.

Privacy and information security training should be mandatory, and agencies need to have, and implement, processes that mandate it. Agencies need to have a policy or procedure that explicitly mandates the training at induction and at regular intervals during employment. They must compel completion of training and engage strategies to monitor and promote progress.



2.2 Results

New and existing QRIDA employees must complete training in information privacy and information security. QRIDA relies on its learning management system to ensure completion of mandatory training. However, QRIDA does not cement these obligations into policies or procedures that explicitly mandate the training.

Recommendation 1 QRIDA

In our 2022-23 audit, we found that QRIDA included information privacy and information security training as part of its induction for new employees. We also found that QRIDA did not require existing staff to undertake refresher training on information privacy and information security.

> *We recommended that QRIDA 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.*

QRIDA has a dedicated learning management system for all new staff at orientation and annual revision training for all employees. It administers new employee and refresher training in four interactive online information privacy and information security modules.[14]

Induction processes are appropriate. They confirm a new employee's obligations to complete training in the information privacy and information security modules. QRIDA automatically enrols new staff in the training modules. These practices demonstrate a proactive approach by QRIDA to make sure that new employees are aware of their training obligations.

However, QRIDA's onboarding checklist, which requires the completion of mandatory courses *by the end of the first week,* does not list any privacy or information security modules as mandatory courses.

QRIDA enrols its staff automatically. They receive enrolment details as well as reminder, overdue and completion notifications for their refresher training.

QRIDA also has procedures that allow it to restrict access to certain information and systems for its new and existing employees. This is a good mitigation strategy to manage access to systems.

New and existing QRIDA employees must complete training in information privacy and information security. During this audit, QRIDA explained that its induction procedures and learning management system make sure that employees are aware of their training obligations and complete their training. This strategy largely depends on the system.

Although current processes to engage new and existing employees to complete the training are good, QRIDA does not have a defining policy or procedure that explicitly mandates training in any of the information privacy and information security modules for its new and existing employees. This represents an opportunity for improvement.

We assess the implementation status of **Recommendation 1** as Partially implemented.

[14] They are Privacy in the workplace; Information Security - Employee awareness; Information Security - Phishing awareness; and Information Security - Social Media.

3 Training material and rollout (Recommendations 2 – 7)

3.1 Introduction

In 2020, the Crime and Corruption Commission reported that education and awareness programs are critical to achieve an effective information privacy culture and promote compliance.[15]

Accurate, appropriate and tailored information privacy and information security training content is a critical part of these programs. 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.

Training should also ensure that employees understand what unauthorised access to personal information is and the consequences of noncompliance. Practical scenarios that relate to the employee's functions and demonstrate how to apply information privacy and information security when undertaking their day-to-day duties are crucial.

Robust assessment also strengthens employees' awareness and understanding of information privacy and information security obligations in their workplace.

Collectively, this content framework supports and embeds standards of behaviour. Without dedicated, accurate and appropriate training content and assessment, training may be ineffective. Wrong or out of date training can even be counterproductive and damaging to the community, the employee and the agency.

Good training material is inconsequential if not rolled out.

3.2 Results - Information privacy training

We made six recommendations about training content and rollout – one to WorkCover and five to QRIDA.

WorkCover has progressively amended, streamlined and strengthened its information privacy training module. It is now a robust information privacy training vehicle.

[15] Operation Impala. Report on misuse of confidential information in the Queensland public sector February 2020. Available at https://www.ccc.qld.gov.au. Accessed 23 April 2025.

QRIDA has made advances since our 2022-23 audit. It rolled out training in information privacy and information security to its employees. Content in these modules is generally good, but there are some gaps and room for improvement.

Figure 6 shows the implementation status of Recommendations 2 – 7 which concern training content and rollout.

Figure 6

Training content and rollout

Recommendation		Status
Recommendation 2	WorkCover includes more comprehensive content on all privacy principles in its information privacy module.	Fully implemented
Recommendation 3	QRIDA develops comprehensive information privacy training content.	Partially implemented
Recommendation 4	QRIDA rolls out training in information privacy for all employees.	Fully implemented
Recommendation 5	QRIDA develops comprehensive information security training content.	Partially implemented
Recommendation 6	QRIDA rolls out training on information security to all employees.	Fully implemented
Recommendation 7	QRIDA 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.	Fully implemented

Source: Office of the Information Commissioner

Recommendation 2 WorkCover

Recommendation 2 concerns WorkCover's information privacy training content.

In our 2022-23 audit, we found that WorkCover's online privacy module provided a good high-level overview of the IP Act and included most of the elements we expected to see, such as defining personal information, outlining the Information Privacy Principles, and explaining how to respond to privacy breaches.

We also identified some gaps.

> *We recommended that WorkCover Queensland 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.*

WorkCover's *Privacy 2024* training module is accurate and consistent with the IP Act. Content about the Information Privacy Principles is thorough and up to date. WorkCover tailors it to its needs.

WorkCover provides access and links to additional resources, such as to the Office of the Information Commissioner website and key internal polices like WorkCover's Information Privacy Policy and Privacy Breach guide. It makes for a more robust module.

Interactive scenarios embed and assess employee knowledge. WorkCover effectively tailors them to its functions, and they are suitable to test employees' understanding of their obligations.

WorkCover has also addressed gaps we identified in its privacy training in our 2022-23 audit. For example:

- a 'Be aware' section about transferring personal information outside of Australia in now included
- it now includes details about who employees can contact if they have questions about information privacy obligations.

We assess the implementation status of **Recommendation 2** as Fully implemented.

Recommendations 3 and 4 QRIDA

Recommendations 3 and 4 concern QRIDA's information privacy training content and the rollout of that training to employees.

In our 2022-23 audit, QRIDA's training material was high level and did not cover all aspects of privacy. For example, we found that while the training gave an overview of the Information Privacy Principles, it did not sufficiently cover all aspects of privacy to properly inform employees of their privacy obligations.

We reported that training did not determine whether the participants understood how privacy applies to them in their day-to-day duties. We did not find any knowledge-based assessment that employees must pass to gain certification for successfully completing the training. We said that there was a risk that employees did not fully understand their information privacy obligations.

We also reported gaps in the rollout of information privacy training. We found that new employees received a link to, and went through, a presentation on compliance obligations which included a high level overview of information privacy (and cyber security). We found no evidence that existing staff received refresher training on a regular basis.

> *We recommended that QRIDA 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.*

and

> *We recommended that QRIDA within twelve months, rolls out training in information privacy for all employees.*

QRIDA has an information privacy training module – *Privacy in the workplace.* It is an online and interactive training module. Some of the content is good, but it is not robust. There is little emphasis and acknowledgement of the IP Act and the Information Privacy Principles. The module also interchangeably uses Commonwealth and Queensland content. There is no explanation provided to employees about why this occurs. This generates significant risk to an employee's understanding of information privacy in Queensland.

QRIDA tailors some aspects of the training module to its unique circumstances. Where this occurs, it reinforces to its employees how and why understanding information privacy is critical. It means that QRIDA employees can link content to their day-to-day duties.

The information privacy training incorporates key messages from the Crime and Corruption Commission’s report into Operation Impala. This means that employees understand the importance of unauthorised access to personal information.

The training module does have assessment to test employee knowledge. However, its effectiveness is somewhat mixed. There are some good and simple elements, but QRIDA could do more to tailor to its unique circumstances and employee functions and reference specific Information Privacy Principles and sections of the IP Act.

There are currently no details of QRIDA’s privacy officer or champion to help employees if they need assistance. QRIDA advised during our audit that it will address this missed opportunity.

QRIDA has rolled out the training. It tells its employees about the rollout in several ways including through all staff emails about the training as well as individual emails from human resources and instructions about how to initialise the training in the learning management system. There are also broadcasts on QRIDA tv.

We assess the implementation status of **Recommendation 3** as Partially implemented.

We assess the implementation status of **Recommendation 4** as Fully implemented.

3.3 Results - Information security training

Recommendations 5 and 6 QRIDA

Recommendations 5 and 6 concern QRIDA’s information security training content and the rollout of that training to employees.

In our 2022-23 audit, we found QRIDA’s training material included information about protecting information and systems on cybersecurity. All employees had access to a recorded cybersecurity training information session. This included new starters.

The video sufficiently informed staff about information security threats and the importance of taking information security seriously. However, it was not mandatory to view the video and QRIDA did not monitor if its employees had watched the presentation.

We found that training materials provided a link to its information security policies located on the intranet. QRIDA said that it takes it on trust that employees read and understand the content of these policies.

This meant QRIDA could not be sure if its staff were familiar with all their information security obligations. Information security training was not an effective tool for mitigating information security risks.

> *We recommended the Queensland Rural and Industry Development Authority 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.*

and

> *We recommended the Queensland Rural and Industry Development Authority within twelve months, rolls out training on information security to all employees.*

QRIDA now has three training modules relevant to information security: Information Security – Employee awareness; Information Security – Phishing awareness; and Information Security – Social Media.

Collectively, these provide QRIDA employees with a good overview of information security, including the threats posed to QRIDA and employee obligations and responsibilities. Referencing and linking to relevant policies in the training modules reflects good practice. It means that employees completing the training can easily navigate between policies and training to strengthen their understanding.

However, there is little if any reference to the IP Act or the Information Privacy Principles, or links to other relevant and important internal policies. There is also no reference in the modules to Information security policy (IS18), which is the primary policy for information security in the Queensland Government.[16] This is a gap and means that employees are not aware of important data and system security obligations.

The training modules do not provide employees with contact details for QRIDA information security and privacy teams if they have any questions about their obligations and responsibilities.

[16] IS18 is available at https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-directions-and-guidance/qgea-policies-standards-and-guidelines/information-security-policy-is18. It is supported by various frameworks, standards, and guidelines under the Queensland Government Enterprise Architecture (QGEA) – see https://www.forgov.qld.gov.au/information-technology/queensland-government-enterprise-architecture-qgea

Some of the training scenarios for employees to consider are practical and often followed by assessment. This is a good strategy and strengthens the training offered. However, there is not enough tailoring. We did see some mirroring in the assessments that would tie to QRIDA employee roles and their day-to-day duties. However, it is generic.

The training modules include assessment to test employee knowledge. They generally cover all the areas you would expect for information security. They are good and accurate, although there is not enough tailoring to the specific workings of QRIDA, the IP Act or the Information Privacy Principles. To be effective, training assessment should link to the Information Privacy Principles that apply to collection, use and disclosure of personal information.

QRIDA has though rolled out its three training modules.

The process and communication strategies are as we reported in Recommendation 4.

We assess the implementation status of **Recommendation 5** as Partially implemented.

We assess the implementation status of **Recommendation 6** as Fully implemented.

Recommendation 7 QRIDA

Recommendation 7 is about including unauthorised access to personal information and the Operation Impala report into its information privacy or information security training modules.

In our 2022-23 audit, we found that QRIDA’s cybersecurity training information video, mentioned that improper use and handling of personal information can affect the agency and its clients. However, it was not explicit enough.

> *We recommended the Queensland Rural and Industry Development Authority 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.*

QRIDA’s Information Privacy training module has a section *Unauthorised Access to Information*. It includes information about the Operation Impala report. It also has explicit information about unauthorised access to information and the potential impacts that such actions can have on:

- the individual whose information was accessed

- the employee inappropriately accessing the information (such as disciplinary action, termination of employment or possible criminal actions)
- the agency.

There are also quizzes to assist employees to understand the topic.

This means QRIDA’s information privacy training module reinforces the expectations around unauthorised access to personal information and conveys the serious potential outcomes of such actions as identified in the Crime Corruption Commission’s Operation Impala Report.

We assess the implementation status of **Recommendation 7** as Fully implemented.

4 Enrolment and monitoring systems and processes (Recommendations 8 – 10)

4.1 Introduction

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

This means agencies must put robust systems and procedures in place to ensure all employees, new and existing, complete the required training by the due date.

4.2 Results

We made one recommendation to each agency about systems and processes to monitor timely training completion for new and/or existing employees.

Overall, we have seen progress and improvements in each agency. Outcomes varied, but there are similarities in approach – for example, automatic enrolment in training, prompts, reminders to employees and their managers and general awareness activities.

However, good frameworks are only effective if staff complete training when it is due.

The Department's systems and processes drive its employees to complete training in information privacy and security. It engages with its employees about the importance and relevance of information privacy and information security in their employment. But training completion is not timely.

WorkCover employees have high and on time completion rates for its information privacy and information security training modules.

QRIDA systems and procedures have improved but not enough. Its monitoring and reporting processes do not ensure that all new and existing employees complete the mandatory training on information privacy and information security when due.

Recommendation 8 Department

Recommendation 8 concerns refresher training for existing employees of the Department.

In our 2022-23 audit, we examined the Department's systems and processes for completing training. We also looked at completion and timing rates for training in the Department's Information Privacy and Cyber Security Essentials training modules. We focused on three areas of the Department – Customer Service, Governance and Human Resources between a specified period.

In our 2022-23 audit, the time provided to complete the training varied – 30 days for employees to complete the privacy training and up to five months to complete the Cyber Security training. When agencies allow lengthy time periods to complete training, such as five months, it increases their exposure to privacy risks and security threats.

Nearly three quarters of employees completed the Information Privacy refresher training by the due date. A higher proportion of existing employees also completed the Cyber Security training by the due date.

Figure 7 below, reproduces data from the 2022-23 audit and shows exiting staff completion rates.

Figure 7
Existing staff completion rates

Training module	Total enrolled	Completed within time	Not completed within time	Proportion completed within time
Information Privacy	1,726	1,232	494	71.4%
Cyber Security Essentials (Jun 2020 to Oct 2020)	1,475	1,387	88	94%
Cyber Security Essentials (Nov 2020 to Dec 2021)	254	223	31	87.8%

Source: Office of the Information Commissioner

These figures suggested that the process for monitoring timely training completion was not working as effectively as it could.

> *We recommended that the Department 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.*

The Department uses its systems and processes to engage and support its employees to complete their training obligations. For example:

- reminder emails sent to employees and managers to prompt on time completion
- monthly Workforce Report data and Dashboards generated and distributed to managers
- regular communication, awareness messages and content across several communication platforms about information privacy and cyber security.

Training completion rates are high – with all but one of the branches examined above 96 percent for completion of both the Cyber Security Essentials training module and the Information Privacy training modules.

However, training completion is not timely. **Figure 8** below, shows existing staff training completion rates for the six month period 1 July 2023 to 31 December 2023.

Figure 8

Existing staff completion rates

Training module	Total enrolled	Completed within time	Not completed within time	Proportion completed within time
Information Privacy	600	312	288	52.0%
Cyber Security Essentials	720	341	379	47.4%

Source: Office of the Information Commissioner

While over 80 percent of employees complete training in each module within one month after the due date, there is still a gap to ensure training is complete when due. It represents risk to what otherwise appear to be good and clear practices.

The Department indicated it is committed to continue promoting best practices in privacy and cyber security. Based on the data received, the measures designed by the Department to make sure employees complete their training in information privacy and information security when due are not working as well as they should.

We assess the implementation status of **Recommendation 8** as Partially implemented.

The Department believes that course completion rates remain consistently good. It considers it has a very good track record in terms of the number and severity of information security incidents and privacy breaches affecting the Department, particularly given its size and decentralised workforce. While this may be the case, the follow-up audit focused on assessing the implementation status of our 2022-23 recommendations.

The Department said that it considers it has met the requirements of the recommendation and it encourages its employees to complete the training within the desired period.

Recommendation 9 WorkCover

Recommendation 9 concerns training for new employees of WorkCover.

In our 2022-23 audit, we said that WorkCover had established processes for enrolling staff in, and monitoring completion of, the information privacy and information security training modules at induction. We found that all new employees must complete 11 mandatory online compliance training modules within 14 days. Three were about privacy and cyber security – Privacy 2021; Contemporary Mobile Workforce 2022; and Technology Use 2021.

Just over half of the new staff completed the modules by the due date. **Figure 9** below, reproduces data from the 2022-23 audit and shows new staff completion rates.

Figure 9

New employees training completion rates

Training module	Total enrolled	Completed within time	Not completed within time	Proportion 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

We found that the rate of completion within 28 days of enrolment in the course was higher, but still not sufficient to ensure all new employees were fully aware of their privacy and cyber security obligations.

These figures suggested that the process for monitoring whether new employees complete the mandatory online training on time was not working as effectively as it could.

> *We recommended that WorkCover implement more robust systems and procedures to ensure all new employees complete the mandatory training on information privacy and information security when due.*

WorkCover assigns, enrols and tells its new employees of their training obligations. This has not changed since our 2022-23 audit. It identifies employees who have not complied with their training requirements and emails the employee and their manager to prompt completion.

New employees now have 30 days to complete the training modules. While this increase from 14 days does marginally raise risk, the 30-day requirement is reasonable and consistent with practices across the sector.

Figure 10 below, shows a comparison of new employees training completion rates for the 2022-23 and 2024-25 audits (*Follow-up audit 2024-2025*, assessed data for the period between January and October 2024).

Figure 10

New employees completion rates

Training module	Initial 2022-23 audit		Follow-up audit 2024-25
	Completed within 14 days	Completed within 28 days	Completed within 30 days
Privacy 2024[17]	59.5%	76.2%	91.7%
Technology and Information Security[18]	52.4%	76.2%	92.5%
Working remotely[19]	50.0%	66.7%	86.2%

Source: Office of the Information Commissioner

[17] Formerly Privacy 2021.
[18] Formerly Technology Use 2021.
[19] Formerly Contemporary Mobile Workforce 2022.

The completion rates have increased considerably since our 2022-23 audit. A very high proportion of WorkCover's new employees complete the training before it is due. This reinforces WorkCover's privacy culture and reduces the likelihood of privacy and information security risks materialising.

We assess the implementation status of **Recommendation 9** as Fully implemented.

Recommendation 10 QRIDA

Recommendation 10 concerns training for new and existing QRIDA employees.

In our 2022-23 audit, we identified a number of limitations in QRIDA's training and enrolment monitoring system and procedures.

We found that QRIDA had a structured induction program that included privacy and information security training. However, employee training data did not capture sufficient information to enable QRIDA to effectively monitor whether new staff complete the training by the due date.

We also found that QRIDA did not require existing staff to undertake regular refresher training in information privacy and information security. The lack of such training meant employees may forget or misunderstand their obligations over time. This exposed QRIDA to greater privacy and information security risks.

We reported that QRIDA had significant work to do to improve how it delivered its education and training to raise employee awareness of their obligations and strengthen its privacy culture.

> *We recommended that QRIDA, within twelve months, implement robust systems and procedures to ensure all new and existing employees complete the mandatory training on information privacy and information security when due.*

QRIDA has taken steps to address our recommendation. It uses a newly rolled out learning management system to drive its employees to complete training in four relevant information privacy and information security modules. It has systems and procedures in place to prompt employees to complete the training modules, such as initial and reminder emails to employees and where necessary, their managers.

QRIDA can also capture data about completion and time of completion, for each of its information privacy and information security training modules. The data records various details, and can capture training:

- enrolment dates
- due dates
- completion dates.

This information is necessary to assess whether employees are completing training when due.

However, the data we received did not include a significant amount of this information (mostly the due date and the completion date). This affected our findings and is a critical flaw that contrasts with other good practices we have observed.

The analysis below is based on the data we received, which is incomplete and unreliable. Nevertheless, we attempted to measure the proportion of employees completing their training modules by the due date.

Figure 11 below, shows employee training completion rates for the six month period 1July 2023 – 31 December 2023.

Figure 11

Employee completion rates

Training module	Total enrolled	Completed within time	Not completed within time	Incomplete data	Proportion completed within time
Privacy in the workplace	200	94	30	76	47%
Information Security - Employee awareness	203	126	68	9	62%
Information Security - Phishing awareness	202	22	44	136	11%
Information Security - Social Media	201	21	45	135	10%

Source: Office of the Information Commissioner

Less than half of employees (47 percent) completed the privacy training before the due date. This is a significant gap.

Nearly two thirds of employees (62.07 percent) completed the training in Information Security – Employee awareness before the due date. This is better, but again, not sufficient to reinforce QRIDA's privacy culture and reduce the likelihood of privacy and information security risks materialising.

Only just over 10 percent of employees complete the Information Security – Phishing awareness and Information Security – Social Media training by the due date. There is significant incomplete data or issues with completion data for these two training modules.

The data also does not differentiate between new and existing employees. It means that new employees may be involved in practices without the required training in information privacy and information security.

QRIDA can customise the time it allows its employees to complete training modules. New and existing employees have the same amount of time to complete the training in each of its modules – there is a one year default. However, the data did not explicitly support this nor show consistent time periods for when training was due. Moreover, providing employees with one year to complete training, significantly increases QRIDA's exposure to information privacy risks and information security threats.

For training strategies to be effective, agencies must put robust systems and procedures in place to ensure all employees, new and existing, complete the required training by the due date. While QRIDA has good induction practices, it cannot demonstrate that all new and existing employees complete the mandatory training on information privacy and information security when due. And the long timeframe, one year, allowed to complete the training, increases QRIDA's risk unnecessarily.

We assess the implementation status of **Recommendation 10** as Some progress.

5 Appendices

Appendix A: Agency responses.

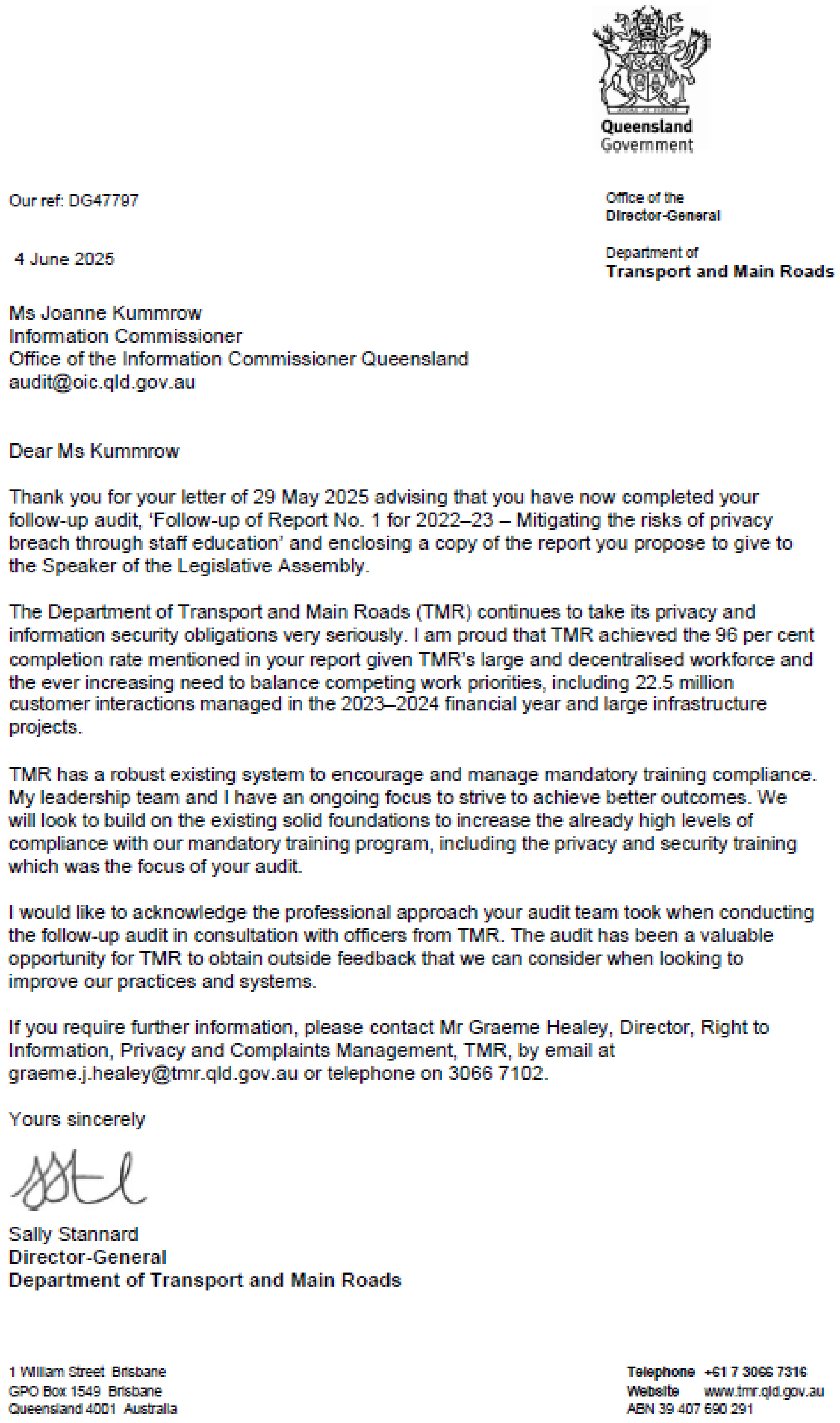
In accordance with our policies and procedures, we provided this report to:

- the Department of Transport and Main Roads
- WorkCover Queensland
- the Queensland Rural and Industry Development Authority,

with a request for comment.

Appendix B - Further details about each agency.

Appendix A – Agency responses



Queensland
Government

Our ref: DG47797

Office of the
Director-General

Department of
Transport and Main Roads

4 June 2025

Ms Joanne Kummrow
Information Commissioner
Office of the Information Commissioner Queensland
audit@oic.qld.gov.au

Dear Ms Kummrow

Thank you for your letter of 29 May 2025 advising that you have now completed your follow-up audit, 'Follow-up of Report No. 1 for 2022–23 – Mitigating the risks of privacy breach through staff education' and enclosing a copy of the report you propose to give 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. I am proud that TMR achieved the 96 per cent completion rate mentioned in your report given TMR's large and decentralised workforce and the ever increasing need to balance competing work priorities, including 22.5 million customer interactions managed in the 2023–2024 financial year and large infrastructure projects.

TMR has a robust existing system to encourage and manage mandatory training compliance. My leadership team and I have an ongoing focus to strive to achieve better outcomes. We will look to build on the existing solid foundations to increase the already high levels of compliance with our mandatory training program, including the privacy and security training which was the focus of your audit.

I would like to acknowledge the professional approach your audit team took when conducting the follow-up audit in consultation with officers from TMR. The audit has been a valuable opportunity for TMR to obtain outside feedback that we can consider when looking to improve our practices and systems.

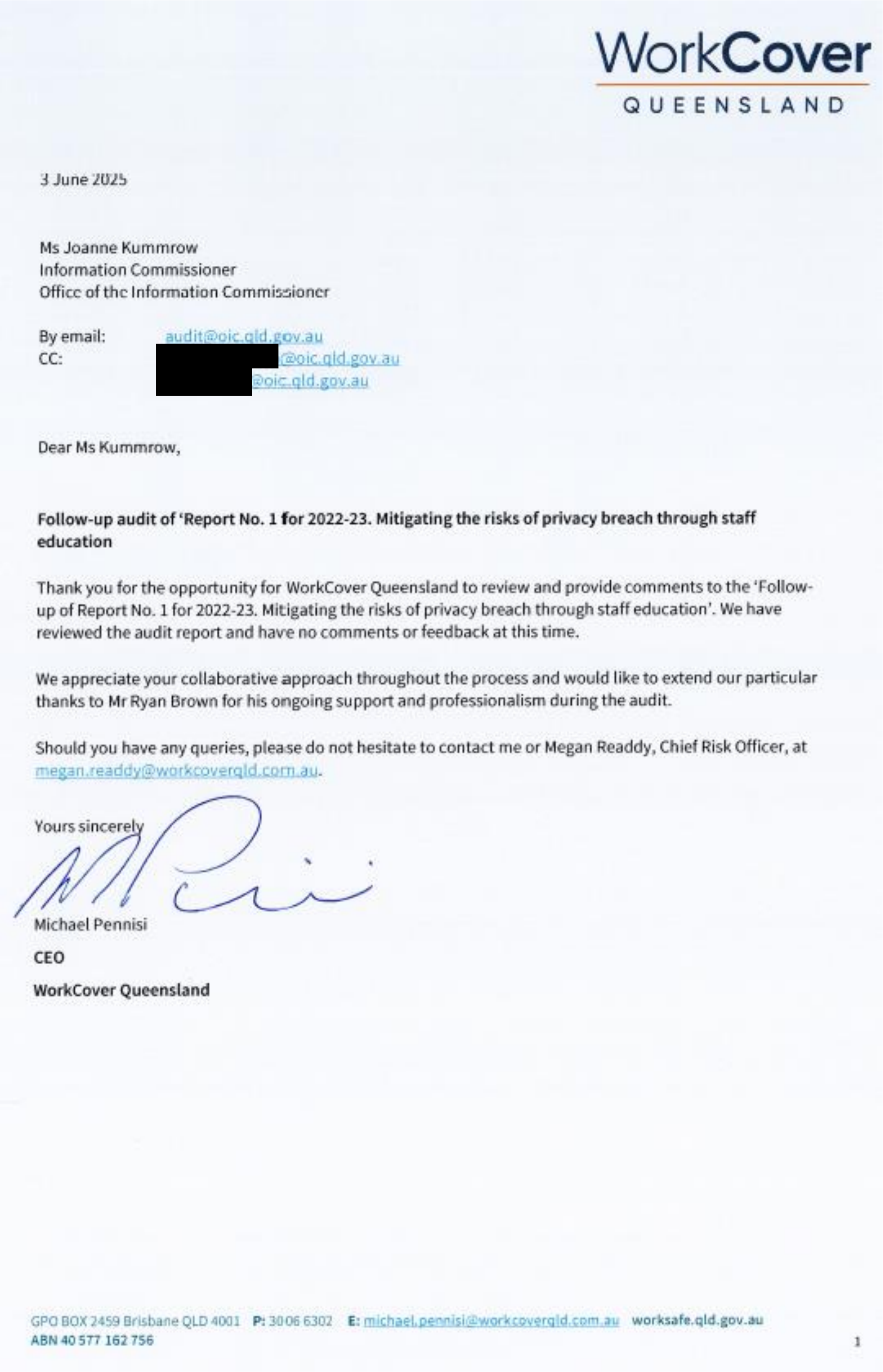
If you require further information, please contact Mr Graeme Healey, Director, Right to Information, Privacy and Complaints Management, TMR, by email at graeme.j.healey@tmr.qld.gov.au or telephone on 3066 7102.

Yours sincerely

Sally Stannard
Director-General
Department of Transport and Main Roads

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



WorkCover
QUEENSLAND

3 June 2025

Ms Joanne Kummrow
Information Commissioner
Office of the Information Commissioner

By email: audit@oic.qld.gov.au
CC: [redacted]@oic.qld.gov.au
@oic.qld.gov.au

Dear Ms Kummrow,

Follow-up audit of ‘Report No. 1 for 2022-23. Mitigating the risks of privacy breach through staff education

Thank you for the opportunity for WorkCover Queensland to review and provide comments to the ‘Follow-up of Report No. 1 for 2022-23. Mitigating the risks of privacy breach through staff education’. We have reviewed the audit report and have no comments or feedback at this time.

We appreciate your collaborative approach throughout the process and would like to extend our particular thanks to Mr Ryan Brown for his ongoing support and professionalism during the audit.

Should you have any queries, please do not hesitate to contact me or Megan Readdy, Chief Risk Officer, at megan.readdy@workcoverqld.com.au.

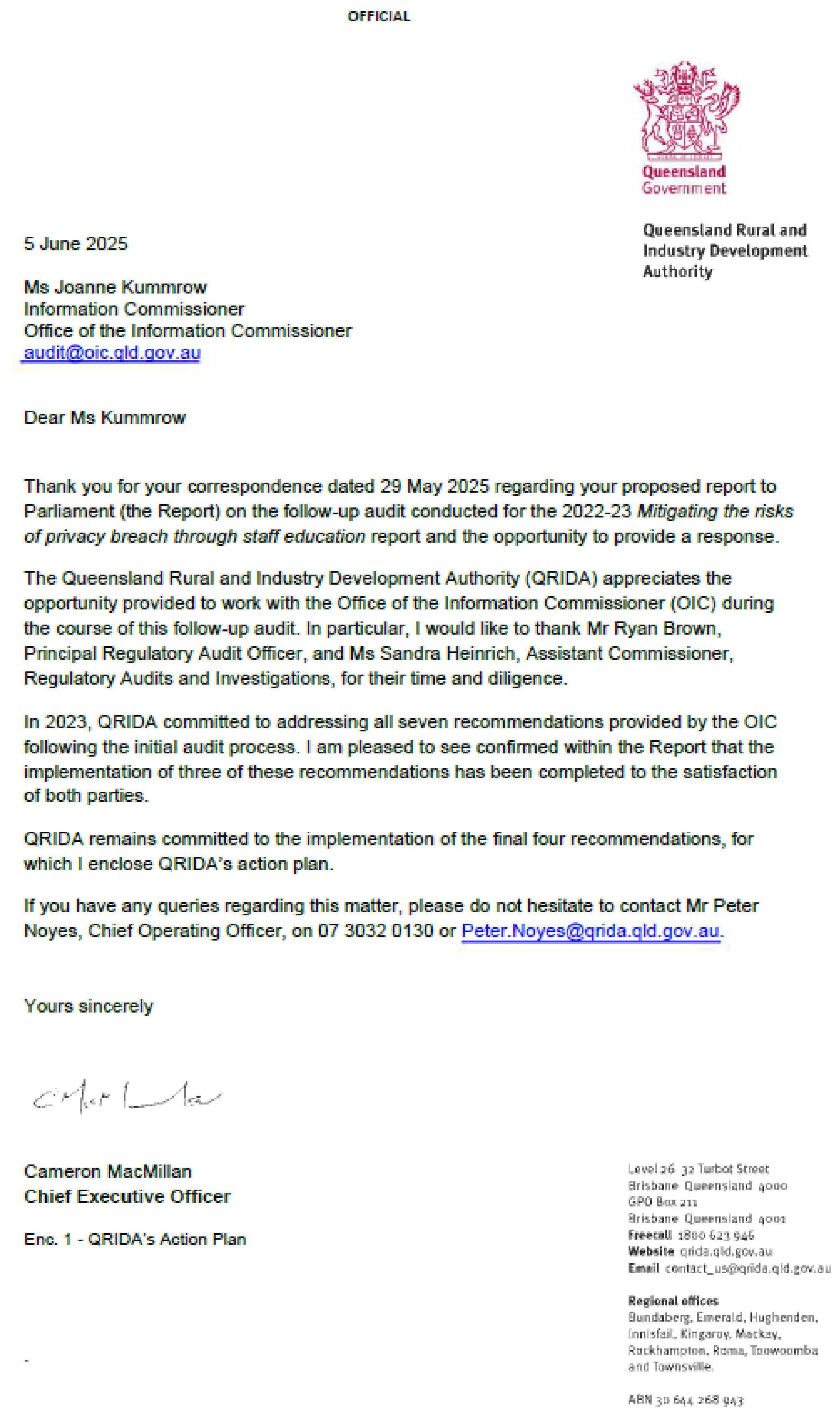
Yours sincerely

Michael Pennisi

CEO

WorkCover Queensland

GPO BOX 2459 Brisbane QLD 4001 **P:** 3006 6302 **E:** michael.pennisi@workcoverqld.com.au **worksafe.qld.gov.au**
ABN 40 577 162 756 1



OFFICIAL

Queensland Government

Queensland Rural and
Industry Development
Authority

5 June 2025

Ms Joanne Kummrow
Information Commissioner
Office of the Information Commissioner
audit@oic.qld.gov.au

Dear Ms Kummrow

Thank you for your correspondence dated 29 May 2025 regarding your proposed report to Parliament (the Report) on the follow-up audit conducted for the 2022-23 *Mitigating the risks of privacy breach through staff education* 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 (OIC) during the course of this follow-up audit. In particular, I would like to thank Mr Ryan Brown, Principal Regulatory Audit Officer, and Ms Sandra Heinrich, Assistant Commissioner, Regulatory Audits and Investigations, for their time and diligence.

In 2023, QRIDA committed to addressing all seven recommendations provided by the OIC following the initial audit process. I am pleased to see confirmed within the Report that the implementation of three of these recommendations has been completed to the satisfaction of both parties.

QRIDA remains committed to the implementation of the final four recommendations, for which I enclose QRIDA's action plan.

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

Enc. 1 - QRIDA's Action Plan

Level 26 32 Turbot Street
Brisbane Queensland 4000
GPO Box 211
Brisbane Queensland 4001
Freecall 1800 623 946
Website qrida.qld.gov.au
Email contact_us@qrida.qld.gov.au

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

ABN 30 644 268 943

Mitigating the risks of privacy breach through staff education report

Audit Action Plan

No.	Office of the Information Commissioner (OIC) Recommendation	Queensland Rural and Industry Development Authority (QRIDA)	Agency comments about progress and implementation	Agency ratings
1	Implement processes that mandate information privacy and information security training: • at induction for all new employees • annual refresher training for all employees.	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.	QRIDA released Learning Management System (LMS) training modules for all new staff upon induction as well as annual revision training for all employees. This process is managed from within the LMS system. The addition to this recommendation from the OIC for a defining policy or procedure is accepted, with QRIDA currently investigating forming an overarching learning and development framework to further develop these implemented processes.	**Partially implemented**
3	Develop 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 employee's knowledge and understanding of the topic • includes details of the agency's privacy officer/champion to assist employees with privacy matters.	QRIDA will establish comprehensive training in QRIDA's LMS for all employees. This training will include employee obligations and responsibilities under the *Information Privacy Act 2009* and relevant policies and test knowledge and understanding of same. QRIDA will also establish protocols relating to unauthorised access to personal information and specific responsibilities under the dedicated privacy officer for QRIDA.	Information Privacy Training has been established within the QRIDA LMS system. Planning for additional updates in accordance with the *Information Privacy and Other Legislation Amendment Act 2023* (IPOLA) has been underway during the course of the OIC IPOLA training delivery timeline, beginning in August 2024.	**Partially implemented**

No.	Office of the Information Commissioner (OIC) Recommendation	Queensland Rural and Industry Development Authority (QRIDA)	Agency comments about progress and implementation	Agency ratings
5	Develop 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.	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 these specialised topics.	Three specialised training LMS modules relating to Information Security: Employee awareness, Information Security: Phishing awareness and Information Security: social media are now mandatory modules for staff completeness upon induction and as part of an annual revision process. These modules will be reviewed for additional information around: • further reference to the *Information Privacy Act 2009* • reference to the Queensland Government Information Security policy (IS18) • information security and privacy team contact details, where appropriate. Further training focused on security threats, obligations, and responsibilities for safeguarding information in accordance with the *Information Privacy Act 2009*, have been iterated and incorporated in regular staff email and newsletter communications.	**Partially implemented**
10	Implement robust systems and procedures to ensure all new and existing employees complete the mandatory training on information privacy and information security when due.	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.	Four specialised training LMS modules relating to Privacy in the Workplace, Information Security: Employee awareness, Information Security: Phishing awareness and Information Security: social media are now mandatory modules for staff completeness upon induction and as part of an annual revision process. Completion timelines for these modules are set at 15 days. Investigations are underway to integrate LMS reporting with existing reporting systems to further refine monitoring of training completion rates.	**Some progress**

Appendix B - Further details about each agency.

Department of Transport and Main Roads

The Department is responsible for planning, managing and delivering an integrated transport network across road, rail, air and sea for the state.

In 2023-24, the department reported that it:[20]

- registered 6 157 512 vehicles registered
- conducted 153 069 written driving tests
- oversaw 178 930 practical driving tests taken
- issued 4 154 952 driver licences
- had 22.5 million customer interactions
- served 8 435 601 million customers face-to-face.

In providing these services, the Department collects and holds a large volume of personal information.

As of 14 June 2024, the Department employed 11 860 employees (full time 8 536, part time 1 257, and casual 206).

WorkCover Queensland

WorkCover Queensland is established under the *Workers' Compensation and Rehabilitation Act 2003* (Qld). Its functions include to provide insurance to businesses in Queensland who employ workers and encourage improved health and safety performance by employers.

In delivering services, WorkCover Queensland in 2023-24:[21]

- responded to 312 767 customer service calls to its contact centre
- insured 179 024 employers
- assisted 74 127 injured workers
- received 3 241 new common law claims.

The personal information WorkCover Queensland collects and holds about a client depends on the service it supplies.

[20] Annual Report 2023-2024. https://www.publications.qld.gov.au/dataset/annual-report-2023-2024-transport-and-main-roads/resource/a4a6d36f-7632-44c1-9367-7352583c16d6

[21] WorkCover Queensland 2023-24 Annual Report available at https://www.worksafe.qld.gov.au/resources/publications/annual-reports/annual-report-2023-2024

As of 30 June 2024, WorkCover Queensland employed 1 095 full time employees.[22]

Queensland Rural Industry Development Authority

QRIDA is a statutory authority established under the *Rural and Regional Adjustment Act 1994* (Qld). It is a specialist administrator of government financial assistance programs including loans, grants and rebates.

It is a specialist administrator of government financial assistance programs including loans, grants and rebates, 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.

It has offices across Queensland, including in Brisbane, Bundaberg, Emerald (with an office in Longreach), Hughenden (with an office in Cloncurry), Innisfail, Kingaroy, Mackay, Rockhampton, Roma, Toowoomba, and Townsville.

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 2023-24, QRIDA reported that it:[23]

- approved 88 933 applications worth more than $343.8 million in government financial assistance
- administered more than $12.8 million through the Queensland Government's Drought Assistance Programs

[22] Excluding Directors, Contractors and Temporary Agency Staff WorkCover Queensland 2023-24 Annual Report available at https://www.worksafe.qld.gov.au/resources/publications/annual-reports/annual-report-2023-2024

[23] Queensland Rural and Industry Development Authority Annual Report 2023-24 available at https://www.qrida.qld.gov.au/sites/default/files/2024-09/QRIDA_annual_report_23-24_Webcopy_PDF865KB.pdf

- helped more than 72 700 households invest in energy-efficient appliances, save an average of $103 on their energy bill, and reduce greenhouse gas emissions by approximately 0.27 tonnes of CO2 a year under the popular Climate Smart Energy Savers Rebate Scheme
- approved 126 applications for $89.1 million were approved for our First Start and Sustainability Loans.

As of 30 June 2024, the authority employed 198.7 full time equivalent employees (127.36 permanent and 71.34 temporary).[24]

[24] Queensland Rural and Industry Development Authority Annual Report 2023-24 page:14 available at https://www.qrida.qld.gov.au/sites/default/files/2024-09/QRIDA_annual_report_23-24_Webcopy_PDF865KB.pdf