Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Applying the legislation – Information Privacy Act 2009

Achieving effective privacy and information security training

This guide does not reflect the current law.

It highlights important changes to the *Information Privacy Act 2009*.

This guide does not constitute legal advice and is general in nature only. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

1.0 Overview

The *Information Privacy Act 2009* (Qld) (**IP Act**) requires agencies[1] to handle personal information in accordance with the Queensland Privacy Principles (QPPs). QPP 11 requires agencies to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure.

2.0 Security strategies

An important part of QPP 11 compliance and reducing privacy and information security risks generally is effective training and education. Agency staff who are effectively trained and understand their obligations help support and maintain a robust privacy culture.[2]

Reports by the OIC and the Crime and Corruption Commission[3] identified key requirements for all Queensland government agencies for effective privacy and information security training, including that it should:

- be mandatory and periodic
- be monitored and followed up to ensure completion
- cover all relevant elements of information privacy and information security
- be accurate and consistent with the IP Act, any confidentiality and security obligations, and relevant policies and procedures
- be practical, contemporary, and tailored to the agency's context; and
- include an assessment component.

[1] Agency includes a Minister, bound contracted service provider or other entity required to comply with the QPPs.
[2] *Report No. 1 for 2018-19, Awareness of privacy obligations* and the *Follow-up of Report No. 1 for 2018-19, Awareness of privacy obligations, Report No. 3* to the Queensland Legislative Assembly for 2020-21 (**the follow-up report**) and the *Crime and Corruption Commission's Operation Impala Report* on misuse of confidential information in the Queensland public sector, tabled in February 2020 (**Operation Impala report**).
[3] The follow-up report and Operation Impala report.

Individual agencies are responsible for implementing OIC recommendations[4] made to all Queensland government agencies, monitoring, and reporting on progress to leadership, and taking appropriate action. OIC will continue to assess agency progress in its audit program and report to Parliament.

2.1 Training must be mandatory and periodic

Privacy and information security training should be mandatory. It forms part of an agency's induction package. Employees should complete it before having access to systems containing personal information.

Mandatory periodic refresher training is just as important. It increases the likelihood of employees retaining their awareness of information privacy and security risks. Agencies can use refresher training to alert staff to any changes in their privacy and information security policies.

By requiring their staff to undertake refresher training periodically, agencies will be able to:

- demonstrate that their employees are aware of their privacy and information security obligations; and
  reinforce an effective privacy culture.

2.2 Training must be monitored and followed-up

For training strategies to be effective, agencies must put robust systems and procedures in place to ensure all employees complete the required training.

2.3 Alternative training delivery

Privacy and information security training is often computer-based, which means agencies must make other arrangements for frontline and other employees who do not have ongoing access to IT networks. Alternative training methods and reminders, such as face to face or self-paced workbooks, must be put in place, along with procedures to report on training completion and follow up as needed.

When a very high proportion of staff complete the training, it reinforces an agency's privacy culture and reduces the likelihood of privacy and information security risks materialising. This goal can be achieved by, for example:

- automatically enrolling employees into training programs
- setting dates by which training must be completed
- sending prompts and email reminders to employees to complete the training when it is due
- copying individual managers into reminder emails sent to employees
- providing regular reports on training completion to management and/or senior executives; and
- ensuring follow up of incomplete training with individual employees.

Examples

[4] *Report No. 1 for 2018-19, Awareness of privacy obligations*.

Agencies have set up the following systems and processes:

- a central learning management system automatically prompts users to complete their training and produces quarterly completion reports for management
- regional human resource teams responsible for generating compliance forward reports to individual managers where necessary; managers are then responsible for following up outstanding training with employees
- a system which automatically enrols employees and prompts them to complete training when due (including employees with limited or no access to the IT network); individual managers are copied into reminder emails sent to staff; and
- senior executives receive quarterly strategic reports on training completion in their areas and business areas follow up incomplete training with individual employees.

2.4 Training needs to target high-risk areas

An important part of effective training is recognising which parts of the agency present greater privacy and information security risks. These might be areas that, for example, handle more sensitive information or use contractors.

In addition to their privacy obligations, many agencies work with legislation that imposes confidentiality obligations on the employees, including after they leave the agency. These obligations need to be addressed in the training, as they represent an area of potential high-risk. Failure to comply can also have significant consequences for employees and the community.

Agencies should address these heightened risks in their training to increase its effectiveness as a risk mitigation strategy.

Example

An agency introduced a mandatory confidentiality obligations module in its induction package. This ensured new employees read and understood their duty of confidentiality. The module clearly defined confidential information and the confidentiality obligations under the agency's legislation.

2.5 Training must be contemporary, practical and tailored to the agency

To be effective, training needs to be comprehensive, contemporary, and relevant to the agency. Agencies can use training packages tailored to their work or offer general privacy and information security training and supplement it with agency specific training.

Whichever option the agency choses, it is important that the training contains practical scenarios that show employees how to apply privacy and information

security principles in their day-to-day duties. Including real-life scenarios and de-identified case studies can be particularly beneficial.[5]

The training content should be up to date and incorporate all aspects of the agency's privacy and information security framework, including relevant privacy and information security policies and procedures.

Chapter 3A of the IP Act establishes a Mandatory Notification of Data Breach (**MNDB)** scheme. Under the MNDB scheme, agencies are obliged to contain, mitigate, assess and provide notification to OIC and particular individuals of eligible data breaches. Agencies are also required to develop and publish a data breach policy. Contemporary agency security training should ensure officers are aware of their obligations under the MNDB scheme, including identifying actual or suspected data breaches, and familiarising officers with the agency's data breach policy. For more information, see ***Mandatory Notification of Data Breach scheme*.**

Examples

As part of developing effective training, agencies have:

- developed a training module that reflects the content of the agency's Information Privacy Plan, including examples of the types of personal information the agency collects, and how the Information Privacy Principles apply to collection, use and disclosure of personal information.
- incorporated detailed scenarios into their training package, specific to the work of the agency, which cover a wide range of situations, including collecting, using and disclosing personal information.
- developed induction training which captures key features of the agency's information security policy, including a detailed list of employee responsibilities, and how to classify and handle information; and
- developed mandatory refresher training that captures key elements of the agency's information security policy, including safeguarding user ID and passwords.

2.6 Training needs to include an assessment

When training includes an assessment component, it increases the likelihood of employees understanding and retaining its content. Requiring employees to test their knowledge as part of the training gives agencies greater assurance that staff are aware of their obligations. It also enhances the effectiveness of training as a risk mitigation strategy.[6]

Example

[5] Operation Impala report.
[6] The follow-up report.

Incorporating a quiz into practical, agency-based scenarios that prompts employees to consider the correct course of action.

3.0 Additional steps

Effective training is only one part of ensuring employees understand their privacy and information security obligations. Awareness raising activities, such as email campaigns and posting information on the agency intranet, are another way to remind employees of their privacy obligations and reinforce appropriate privacy behaviours in their everyday work.

Examples

- A series of short 'did you know' articles, published on the agency intranet home page, which includes practical privacy topics, such as misdirected emails, shredding documents, floor security and privacy impact assessments.
- Using all-staff emails and intranet campaigns to promote the agency's privacy and information security policies, including the development of a virtual cyber security champion, promoting information security in various online channels.

For additional IPOLA assistance, please contact the IPOLA team by email IPOLA.Project@oic.qld.gov.au

For information and assistance on current legislation, please refer to the OIC's guidelines, or contact the Enquiries Service on 07 3234 7373 or by email enquiries@oic.qld.gov.au

Published August 2024 and Last Updated 22 August 2024