Applying the legislation

GUIDELINE *Information Privacy Act 2009*

Managing privacy in a pandemic

Queensland government agencies[1] must collect, store, use and disclose personal information[2] in accordance with the privacy principles[3] contained in the *Information Privacy Act 2009* (Qld) (IP Act). This guideline is intended to assist agencies to manage their privacy obligations when dealing with some common issues that have arisen during the pandemic.

Agencies may also find these guidelines useful:

- *Privacy and managing disaster events*
- *Privacy flexibility in disaster management - information sharing scenarios*

Can we use staff emergency contact information to notify them of office closures or emergencies?

Yes. Emergency contact information can be used during a pandemic to communicate important messages and for agency business continuity plans. This could include messages about changes to operational requirements, such as office closures, or giving staff information about an emergency.

It is important that emergency contact details are kept up to date.[4] Agencies should consider a regular reminder (eg annually or twice-yearly) that staff update personal and emergency contact details.

Can we tell our staff that they may be at risk because a colleague or visitor has been exposed to a virus such as COVID-19?

Yes, if you believe notification is necessary to ensure the health and safety of staff, visitors, or the public. This is because the privacy principles allow personal information to be used to lessen or prevent a serious threat to someone's life or to the health, safety, or welfare of an individual or the public.[5]

Telling staff that a work colleague has tested positive for—or has come into contact with someone who tested positive for—the virus means the staff can take steps to, protect themselves or self-isolate, and be alert for symptoms. In some circumstances this may require identifying the specific individual, for example to notify someone who was in direct contact with them and while this is

[1] Agency includes a Minister
[2] Any information about an individual whose identity can reasonably be ascertained. See section 12 of the IP Act.
[3] These include the Information Privacy Principles (IPPs) for non-health agencies, the National Privacy Principles (NPPs) for health agencies, and section 33 for both, which regulates the transfer of personal information out of Australia.
[4] IPP 8 requires non-health agencies, and NPP 3 requires health agencies, to take reasonable steps to ensure personal information is accurate and up to date before it is used. IPP 3 also requires non-health agencies to take reasonable steps to ensure personal information they collect is up to date.
[5] IPP 10(1)(b), if the agency is satisfied on reasonable grounds use is necessary and NPP 2(1)(d), if the health agency reasonably believes that the use is necessary.

permitted under the privacy principles agencies should avoid doing so unless necessary.

This will only apply to information about a staff member or a visitor who attended the office. If a staff member tested positive post-holiday and has not yet returned to the office, staff do not need to be notified as they could not have been exposed.

Notifying a visitor to the office

If a visitor to the office was exposed to a staff member or another visitor who tested positive, or was exposed to someone who tested positive, they can also be notified. Details of the individual should not be provided, unless it is impossible to notify without doing so.[6]

We are implementing working from home arrangements for staff - what are the privacy considerations for this?

Where agencies transition to working remotely due to office closures, limiting office attendance, or other pandemic-related reasons, all staff must continue complying with both their privacy and information security obligations and any agency-specific information policies and procedures. It is important that agencies ensure staff:

- continue complying with the privacy principles when collecting, storing, using and disclosing personal information
- use appropriate security on any devices used for official agency business or containing agency information
- secure mobile devices such as laptops and mobile phones used for official agency business or containing agency information against theft or loss
- conduct their work in private to ensure the security of information.

Agencies may want to give staff a copy of the *Protecting personal information when working remotely* tip sheet.

If they do not already have them, agencies will need to develop remote working procedures that suit their specific needs. These should include the requirement that devices permitted to remotely access agency systems have:

- necessary security software installed;
- multi-factor authentication log in;
- appropriate cyber security in place; and
- been set up to use trusted network or cloud services.

[6] Under IPP 11(1)(c) and NPP 2(1)(d) disclosure of personal information to prevent a threat to the life of an individual or to the health, safety, or welfare of an individual or the public is permitted on the same grounds as use (see above).

If staff are permitted to use their own devices for official agency business agencies need to make sure staff meet both their privacy obligations and their public records obligations. These could be addressed in a 'bring your own device' policy, which agencies should ensure covers staff working remotely using their own devices. The policy *Using portable storage devices* may be useful.

Privacy Impact Assessments

Privacy impact assessments help an agency assess the privacy risks involved in new activities. They can also assist in the creation of workplace policies and procedures, including large portions of an agency's staff working remotely. Please refer to *Overview of the Privacy Impact Assessment (PIA) process* for more information.

A staff member has applied for government assistance – do I need their agreement to disclose information to the government body assessing their eligibility?

Disclosing personal information with the staff member's consent is the preferred means for respecting their privacy and complying with the privacy principles,[7] and many government assistance schemes require applicants to consent to the collection of their information. Where the agency has the staff member's (or former staff member's) consent, the agency must be careful to disclose only the information that is covered by their consent, and not any additional information.

In some circumstances, the body administering the assistance scheme may have power under an Act to require the agency to give them information. Where such a power exists, and the body exercises it correctly, the consent of the staff member is not required to disclose their information.[8] The agency may also wish to discuss with the body whether it would be appropriate to tell the staff member that the agency has disclosed their information and to whom.

Can we collect personal information to comply with Public Health Directions without breaching the privacy principles?

Public Health Directions (Direction) have the force of law. If a Direction[9] requires operators of certain kinds of business to collect the personal information of attendees, and if an agency is operating that kind of business, it must comply with the Direction. Doing so does not breach the privacy principles. In order to comply with their privacy obligations, the agency will be required to include the Direction in their collection notice.[10]

[7] IPP 11(1)(b) for non-health agencies, which refers to agreement, and NPP 2(1)(b) for health agencies, which refers to consent.
[8] IPP 11(1)(d) for non-health agencies: disclosure is authorised or required under a law; NPP 2(1)(f): the disclosure is authorised or required by or under a law.
[9] https://www.health.qld.gov.au/system-governance/legislation/cho-public-health-directions-under-expanded-public-health-act-powers/business-activity-undertaking-direction#:~:text=Citation,Direction%20(No.%205).
[10] Under IPP 2 for non-health agencies, and NPP 1 for health agencies, certain information must be given to an individual when their information is being collected, including any authority for the collection.

Some individuals may feel uncomfortable providing this information. The agency may wish to explain that the information is being collected to help protect their health and that operating the business without collecting it would be breaking the law.

For additional information and assistance please refer to Privacy and Public Service Employees during the pandemic and the information sheet Your privacy rights in a pandemic or contact the Enquiries Service on 07 3234 7373 or email enquiries@oic.qld.gov.au.

This guide is introductory only, and deals with issues in a general way. It is not legal advice. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

If you have any comments or suggestions on the content of this document, please submit them to feedback@oic.qld.gov.au.

Published 9 March 2021 and Last Updated 9 March 2021

Changes to legislation after the update date are not included in this document