



**Office of the Information Commissioner**  
Queensland

## **Privacy in complaint handling systems**

A review of how privacy obligations in the *Information Privacy Act 2009* (Qld) have been incorporated in Queensland government agencies' complaint handling systems

OIC thanks agencies for their cooperation throughout the review and for the courtesy displayed towards the officers conducting the assessment.



This report to the Queensland Legislative Assembly by the Office of the Information Commissioner is licensed under a Creative Commons – Attribution License. People reading or using this report may do so in accordance with the following conditions: Attribution (BY), requiring attribution to the original author.

© The State of Queensland (Office of the Information Commissioner) 2014

Copies of this report are available on our website at [www.oic.qld.gov.au](http://www.oic.qld.gov.au) and further copies are available on request to:

Office of the Information Commissioner  
Level 8, 160 Mary Street, Brisbane, Qld 4000  
PO Box 10143, Adelaide Street, Brisbane, Qld 4000

Phone 07 3234 7373  
Fax 07 3405 1122  
Email [administration@oic.qld.gov.au](mailto:administration@oic.qld.gov.au)  
Web [www.oic.qld.gov.au](http://www.oic.qld.gov.au)

ISBN: 978-0-646-91917-1

March 2014

The Honourable Fiona Simpson MP  
Speaker of the Legislative Assembly  
Parliament House  
George Street  
BRISBANE Q 4000

Dear Ms Speaker

I am pleased to present 'Privacy in complaint handling systems: A review of how privacy obligations in the *Information Privacy Act 2009* (Qld) have been incorporated in Queensland government agencies' complaint handling systems.' This report is prepared under section 135 of the *Information Privacy Act 2009* (Qld).

The report reviews personal information handling practices, in particular compliance with the Information Privacy Principles, which agencies are required to adopt under section 27 of the *Information Privacy Act 2009* (Qld). It highlights examples of good privacy practice already adopted by some agencies and publicises the availability of further privacy resources.

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

Yours sincerely

A handwritten signature in dark ink, appearing to read 'Rachael Rangihaeata'.

Rachael Rangihaeata  
**Information Commissioner**



## Table of Contents

<b>1</b>	<b>Executive Summary .....</b>	<b>1</b>
<b>2</b>	<b>Summary of Findings.....</b>	<b>3</b>
<b>3</b>	<b>Introduction .....</b>	<b>8</b>
	3.1 Background	8
	3.2 Description of a Complaints Management System (CMS)	9
	3.3 Legislative requirements – the Information Privacy Act	9
	3.4 Scope and objectives	11
	3.5 Assessment process	11
<b>4</b>	<b>Receiving complaints .....</b>	<b>13</b>
	4.1 Fair collection and handling of personal information	15
	4.2 Complaint forms	19
	4.3 Collection notices	21
	4.4 Allowing complaints to be made anonymously	24
	4.5 Limiting the collection of personal information to relevant information	27
	4.6 Training and awareness	29
<b>5</b>	<b>Recording complaints.....</b>	<b>31</b>
	5.1 Registering complaints	33
	5.2 Recordkeeping requirements	35
	5.3 Storage and security of complaint information	37
	5.4 Acknowledging receipt of a complaint	39
<b>6</b>	<b>Processing complaints .....</b>	<b>41</b>
	6.1 Natural justice	43
	6.2 Interviewing witnesses and other third parties to a complaint	45
	6.3 Contracted Service Providers	47
<b>7</b>	<b>Responding to complaints .....</b>	<b>49</b>
	7.1 Communicating the outcome of a complaint	49
	7.2 How much detail should be given about the outcome or decision?	51
	7.3 Access applications under the Right to Information Act 2009 (Qld)	53
<b>8</b>	<b>Management reporting on complaints .....</b>	<b>55</b>
	8.1 Collecting personal information for a secondary purpose	56
	8.2 Use of case notes	58
	8.3 Personal information holdings	59
<b>9</b>	<b>Conclusion.....</b>	<b>61</b>

<b>APPENDICES.....</b>	<b>63</b>
Appendix 1 – Acronyms	65
Appendix 2 – Terms of Reference	67
Appendix 3 – Referral of a complaint to another agency fact sheet	69
Appendix 4 – Sample complaint form	71
Appendix 5 – Sample complaint intake form	75
Appendix 6 – Sample complaints register	77
Appendix 7 – Sample complaints information sheet template	79
Appendix 8 – Sample contract provisions	81
Appendix 9 – Information Privacy considerations when responding to complaints about employees fact sheet	83
Appendix 10 – Scenarios: Providing information on outcomes	85
Appendix 11 – Sample performance reporting template	89
Appendix 12 – Identifying systemic issues, significant issues and trends fact sheet	91
Appendix 13 – Further complaint handling resources	95

# 1 Executive Summary

---

Community dissatisfaction with some government decisions and actions is inevitable. This can lead to complaints. Properly handled, complaints handling processes can be an effective way of promoting accountability and transparency in government and can provide information that can assist in improving service delivery.

Inefficient and ineffective complaint handling can disproportionately consume agency resources and time; adversely affect the agency's reputation; and cause or increase distress to a complainant. Inadequate complaint handling also increases the likelihood the complainant will pursue relevant issues in court, tribunal proceedings or investigations by other review bodies.

There are various elements in effective complaint handling. One essential element is respect for the privacy of individuals involved in a complaint.

This review looked at the extent to which privacy considerations are incorporated into agencies' Complaints Management Systems (**CMS**). The intent of the review was not to identify weaknesses in any particular agency CMS but rather, to identify areas of good privacy practice that could be publicised as a resource for others.

The Office of the Information Commissioner (**OIC**) commenced the review by conducting a desktop audit of a sample of agency websites to identify the extent to which privacy considerations were incorporated into publicly-available agency complaint handling policies and practices.

The desktop review found that the sampled agencies' complaint handling policies and procedures included explicit mention of privacy, but that this was often limited to a statement that personal information would be managed in accordance with the *Information Privacy Act 2009* (Qld) (**IP Act**). Limited guidance was publicised on how this would be achieved.

The desktop review led to the selection of six agencies for an in-depth review; the agencies were selected on the basis of the quality of their complaint handling documentation available online.

This report showcases the good privacy practices of these agencies.

A secondary objective of the review was to identify resources agencies could use to encourage greater compliance with the IP Act when handling a complaint. OIC recognises the value of formal documented processes in achieving consistency and quality of outcomes.

This report identifies resources to assist agencies in ensuring that CMSs provide safeguards for the collection and handling of an individual's personal information through compliance with the requirements of the IP Act.

An overall recommendation is that agencies review their CMSs and incorporate the good privacy practices outlined in this report.



## 2 Summary of Findings

The following table sets out good privacy practices of the agencies which were the subject of the in-depth review, with associated legislative references and relevant Office of the Information Commissioner (**OIC**)<sup>1</sup> resources.<sup>2</sup> It is recommended that agencies review their Complaints Management Systems (**CMS**) to incorporate these good privacy practices.

This review consistently refers to the Information Privacy Principles (**IPPs**), because the six agencies featured are subject to the IPPs. However, the discussion on good privacy practices equally applies to health agencies. Accordingly, the table references in brackets the equivalent National Privacy Principles (**NPPs**) to the discussed IPPs.

**Table 1: Key findings**

	<b>Legislative requirements<sup>3</sup> OIC Guidelines and Resources</b>	<b>Good privacy practice identified in the in-depth review</b>
<b>Receiving complaints</b>	Collection of personal information <i>IPP1 to IPP3</i> ( <i>NPP1</i> )  Anonymity <i>IPP1</i> ( <i>NPP8</i> )	<i>Privacy considerations made explicit</i> <ul style="list-style-type: none"><li>• There was explicit mention of privacy in complaint handling policy and procedures.</li><li>• Clear advice was provided to the community about the circumstances where the agency's complaints management policy applied, with easy access to further information about those complaints with different management processes.</li><li>• Consent was sought from the individual before referring a complaint to a different agency.</li></ul>

<sup>1</sup> 'OIC' is the Office of the Information Commissioner – a full list of acronyms is provided in Appendix 1.

<sup>2</sup> Office of the Information Commissioner privacy resources are available from [www.oic.qld.gov.au](http://www.oic.qld.gov.au).

<sup>3</sup> Information Privacy Principles (**IPPs**) or National Privacy Principles (**NPPs**).

Legislative requirements <sup>3</sup> OIC Guidelines and Resources	Good privacy practice identified in the in-depth review
<p><b><u>OIC guidelines and resources:</u></b></p> <ul style="list-style-type: none"> <li>• Complaints – collection, storage and security of personal information (identified for development)</li> <li>• Anonymity, confidentiality and privacy in complaints (identified for development)</li> <li>• Demographics and privacy; and</li> <li>• Privacy complaints management online training.</li> </ul> <p>Collection Notices IPP2 (NPP1(3))</p>	<p><i>Only relevant personal information sought from complainants</i></p> <ul style="list-style-type: none"> <li>• Information was asked for in such a way to minimise the collection of irrelevant information.</li> <li>• The complaints form was limited to the collection of relevant information, with mandatory information clearly indicated.</li> <li>• Where appropriate, complaints could be made anonymously.</li> </ul> <p><i>Notices given about use of information</i></p> <ul style="list-style-type: none"> <li>• ‘Collection notices’<sup>4</sup> were provided through a variety of ways, for example, statements on forms and web pages, fact sheets and call handling scripts.</li> <li>• Collection notices went beyond the strict obligations in the privacy principles to provide fuller information on the potential information flows in the course of the complaint process.</li> <li>• Acknowledgement of complaints was used as an opportunity to formally provide complainants with a collection notice as well as provide information about how an agency managed, used and disclosed personal information collected throughout the handling of a complaint.</li> </ul>

<sup>4</sup> A collection notice is the term used to describe the information provided by an agency to an individual satisfying the requirements of IPP2.

	Legislative requirements <sup>3</sup> OIC Guidelines and Resources	Good privacy practice identified in the in-depth review
		<p><i>Good management and record-keeping, awareness of privacy</i></p> <ul style="list-style-type: none"> <li>• A system was in place for identifying, recording and reporting privacy complaints.</li> <li>• Staff received training on the agency's CMS which included a component on the identification of privacy considerations in complaint handling.</li> </ul>
Recording complaints	<p>Storage and security of personal information <i>IPP4</i> (<i>NPP4</i>)</p> <p>Accurate, complete and up to date <i>IPP8</i> (<i>NPP3</i>)</p> <p><b><u>OIC guidelines and resources:</u></b></p> <p>Complaints – collection, storage and security of personal information (identified for development)</p>	<p><i>Information capture and flow controlled</i></p> <ul style="list-style-type: none"> <li>• A centralised or standardised Complaints Register was used to track and monitor complaints.</li> <li>• Guidance was provided to staff on what information must be created and captured in the agency's recordkeeping system for a full and accurate record to be made of the complaint.</li> <li>• Appropriate measures were taken to safeguard complaints documents against unauthorised access, use, modification or disclosure.</li> </ul>

	Legislative requirements <sup>3</sup> OIC Guidelines and Resources	Good privacy practice identified in the in-depth review
Processing complaints	<p>Collection of personal information <i>IPP1 to IPP3</i> (<i>NPP1</i>)</p> <p>Disclosure of personal information <i>IPP11</i> (<i>NPP2</i>)</p> <p>Contracted Service Providers <i>Chapter 2, Part 4</i> (<u>applies to all agencies</u>)</p> <p><b><u>OIC guidelines and resources:</u></b></p> <ul style="list-style-type: none"> <li>• Privacy in complaints management: Disclosure of personal information and natural justice (identified for development)</li> <li>• Contracted service providers; and</li> <li>• Privacy complaints management online training</li> </ul>	<p><i>Complaint handling procedures respectful of privacy</i></p> <ul style="list-style-type: none"> <li>• Parties to the complaint were given appropriate collection notices.</li> <li>• All reasonable steps were taken to bind contracted service providers to compliance with the privacy principles where the service arrangements involved handling or investigating complaints on behalf of the agency.</li> </ul>
Responding to complaints	<p>Use and disclosure of personal information <i>IPP10 and IPP11</i> (<i>NPP2</i>)</p> <p><b><u>OIC guidelines and resources:</u></b></p> <ul style="list-style-type: none"> <li>• Investigations, outcomes and complainants</li> <li>• Applications for investigation and complaint documents; and</li> <li>• Applying for complaint documents</li> </ul>	<p><i>Complaints resolved in a way respectful of privacy</i></p> <ul style="list-style-type: none"> <li>• Witnesses and other third parties to a complaint were given collection notices prior to being interviewed.</li> <li>• Agencies were open and transparent about the potential use and disclosure of information collected during interviews.</li> <li>• Interviewees were either provided with a copy of recordings (as appropriate) upon request or given the opportunity to verify the accuracy of a written record of interview.</li> <li>• Agencies understood the need to afford natural justice including an understanding of and adherence to the permissions and limitations of natural justice.</li> </ul>

	Legislative requirements <sup>3</sup> OIC Guidelines and Resources	Good privacy practice identified in the in-depth review
Management Reporting on complaints	<p>Use and disclosure of personal information <i>IPP10 and IPP11</i> <i>(NPP2)</i></p> <p>Providing information about personal information held by an agency <i>IPP5</i> <i>(NPP5)</i></p> <p><b><u>OIC guidelines and resources:</u></b></p> <ul style="list-style-type: none"> <li>• Case notes</li> <li>• Dataset publication and de-identification techniques; and</li> <li>• Personal information holdings (identified for development)</li> </ul>	<p><i>Information about complaints used and disclosed appropriately</i></p> <ul style="list-style-type: none"> <li>• Policies and procedures were in place to ensure that personal information obtained in the course of the complaint was disclosed and/or used for secondary purposes and only as provided for in the IP Act.</li> <li>• Complaints data was appropriately de-identified before the data was used for a secondary purpose, such as performance monitoring.</li> <li>• If complaints data was reported on or used for training and guidance purposes, it was appropriately de-identified.</li> <li>• Information about the type of personal information contained in complaints documents and the main purposes for which this personal information was used was included in the agency's list of personal information holdings.</li> </ul>

## 3 Introduction

---

### 3.1 Background

The Queensland State Government has consistently given a commitment for public sector agencies to be open, accountable and responsible to the community. As part of this ethos, agencies should handle complaints in a manner that is respectful of the privacy of the parties to the complaint.

In Queensland and in other jurisdictions, the community is becoming more privacy-aware and concerned that government recognises and respects individual's privacy. For example, a survey conducted in 2013 by the Office of the Australian Information Commissioner on community attitudes to privacy showed that an increasing majority of people (82% compared with 69% in 2007) claimed to be aware of federal privacy laws. The survey also found a slight decrease in the level of community trust in the way that government departments handle personal information (69% down from 73% in 2007).<sup>5</sup>

Other research has found that the community believes privacy to be important and expects government to build privacy considerations into agency websites.<sup>6 7</sup> An agency which does this demonstrates to the community that the agency is addressing their concerns about privacy.

Queensland's Office of the Information Commissioner (**OIC**) has a responsibility under Chapter 5 of the *Information Privacy Act 2009* (Qld) (**IP Act**) to deal with privacy complaints made against Queensland government agencies through mediation.<sup>8</sup> An individual who believes an agency has not dealt with their personal information in accordance with the privacy principles set out in the IP Act may make a privacy complaint

---

<sup>5</sup> OAIC *Community Attitudes to Privacy survey* Research Report 2013 viewable at [http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/Final\\_report\\_for\\_WEB.pdf](http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/Final_report_for_WEB.pdf)

<sup>6</sup> For example, a recent telephone survey of 2,000 Canadian adults found:  
*More than three quarters (77%) felt it to be very important that websites actively inform users about what kinds of personal information they are collecting and how they use it.*  
*2011 Canadians and Privacy Survey, Report, Presented to the Office of the Privacy Commissioner of Canada, March 31, 2011, page 3, viewed at [https://www.priv.gc.ca/information/por-rop/2011/por\\_2011\\_01\\_e.pdf](https://www.priv.gc.ca/information/por-rop/2011/por_2011_01_e.pdf) on 7 August 2013.*

<sup>7</sup> The Public Service Commission, *Discussion Paper: Innovations in ICT for Improving Service Delivery: e-Government* (2010) <http://www.psc.qld.gov.au/publications/subject-specific-publications/assets/ict-and-sd-paper-for-feb-board-4-feb.doc> viewed on 5 March 2014, showed that Queenslanders expect authoritative and reliable information, security in their online interactions and for government to respect their privacy.

<sup>8</sup> Under section 18 of the IP Act, an agency (other than for chapter 3 of the IP Act) means a department, Minister, local government or public authority.

to the agency concerned. If, after 45 business days, they are dissatisfied with an agency's response they may bring their complaint to OIC.

Against this background of increasing community awareness regarding privacy related matters, two factors led to OIC deciding to conduct this review. Firstly, a significant number of privacy complaints lodged with OIC arose from a perception that personal information had been misused during an agency's management of another complaint.

Secondly, agency feedback was that more privacy-related guidance material in the area of complaints management was required.

For example OIC has noted that a common subject of privacy complaints lodged with it is the differing perceptions of complainants and agencies on where the line is between ensuring anonymity and confidentiality and the requirements to provide natural justice and procedural fairness.

### **3.2 Description of a Complaints Management System (CMS)**

A Complaints Management System (**CMS**) means the policy, procedures, personnel and technologies used by an agency in receiving, recording, responding to and reporting about complaints.<sup>9</sup> An effective CMS can increase client satisfaction and enable an agency to review its own performance by identifying areas where business processes and systems can be improved.

### **3.3 Legislative requirements – the Information Privacy Act**

The IP Act came into force on 1 July 2009 (1 July 2010 for local government). The IP Act sets out privacy principles which agencies must comply with when they collect, store, use and disclose personal information. This obligation applies in the course of managing complaints, which will invariably involve personal information.

---

<sup>9</sup> The term 'Complaints Management System' has been adopted for the purposes of this review as this term was used in *Directive 13/06 – Complaints Management Systems*. Although this directive was repealed on 9 August 2013, the Public Service Commission has advised that they will be exploring other mechanisms to confirm the responsibility of agencies to have effective complaints management systems in place and in the interim, agencies are expected to maintain their existing complaints management systems. For further information, please refer to the extract from a whole-of-government communique viewable at <http://www.ombudsman.qld.gov.au/PublicAgencies/Resources/EffectiveComplaintsManagement/ComplaintsManagementResources/tabid/93/Default.aspx>

‘Personal information’ is defined in section 12 of the IP Act as:

***Personal information** is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*

**Examples of personal information arising in the course of a complaint:**

- Names, contact details and personal circumstances of complainants
- Names, contact details and personal circumstances of persons who are the subject of the complaint
- Names, contact details and personal circumstances of witnesses, expert advisers or otherwise involved third parties to the complaint
- Name, contact details and opinions of persons investigating the complaint; or
- Information about the outcome of a complaint made against an individual including what disciplinary action may have been taken against the subject of the complaint.

It is not necessary that the information directly disclose the identity of the individual to be considered as personal information. There may be circumstances where an individual’s identity is ‘reasonably ascertainable’ from the content or context in which the complaint has arisen, even though the complaint may have been made anonymously. For example, if a complaint was made about a staff member’s behaviour, the identity of the complainant could be easily ascertained if the complaint detailed incidents where there were few other individuals involved.

An agency’s privacy obligations are set out in Chapter 2 of the IP Act. This chapter requires an agency<sup>10</sup> to comply with either the Information Privacy Principles (IPPs)<sup>11</sup> or in the case of health agencies, the National Privacy Principles (NPPs).<sup>12</sup> Chapter 2 also provides rules dealing with transferring personal information out of Australia and bound contracted service providers.

This review consistently refers to the IPPs, in part because the six agencies featured are subject to the IPPs. However, the privacy obligations under the NPPs are substantially

<sup>10</sup> All references to agencies includes bound contracted service providers.

<sup>11</sup> Applies to agencies, which includes a Minister, department, local government and public authority.

<sup>12</sup> Applies to health agencies.



similar to the IPPs and the identified good privacy practices equally apply to health agencies.

An exception is NPP8, which explicitly sets out that individuals must have the option of not identifying themselves when entering into transactions with a health agency, wherever this is lawful and practical. There is no direct equivalent to NPP8 in the IPPs. However, IPP1(1)(b) requires the agency to collect only necessary personal information. If the identity of the complainant is not necessary for the administration of the complaint, anonymity should be afforded the complainant.

### **3.4 Scope and objectives**

The review examines and reports on the extent to which Queensland government agencies' complaint handling systems incorporate privacy considerations and adopt the privacy principles set out in the IP Act.

The objectives are to publicise examples of good practice, and identify areas of complaint practice requiring the development of privacy themed information resources.

The Terms of Reference are provided in Appendix 2.

### **3.5 Assessment process**

OIC conducted a 'desktop audit' of the publicly-available information about complaints management on websites of 38 agencies – comprising 21 government departments, the ten largest local councils<sup>13</sup> and seven universities, to identify agencies with a superior approach to the incorporation of privacy obligations in their CMS.

A desktop audit is a scan of an agency's website. The audit analysed the extent to which privacy considerations had been incorporated into complaint handling material and assessed against factors such as:

- whether or not a complaints management policy was available and the extent to which the policy mentioned privacy
- the ways in which individuals were asked to provide personal information
- the extent to which the complaints process limited the collection of personal information to relevant information

---

<sup>13</sup> Selected by analysing rate revenue in 2011/12, the number of full time equivalent staff employed by each Council in 2011/12 and the resident population in 2012.

- whether or not a complaint could be made anonymously; and
- the extent to which material notified the parties to the complaint about the use and disclosure of personal information in the complaint process.

Following this initial scan, the following agencies were selected for in-depth examination, based on the identified superior quality of their online complaint handling material:

- City of Gold Coast
- Central Queensland University (**CQUniversity**)
- Department of Justice and Attorney-General (**DJAG**)
- Department of Science, Information Technology, Innovation and the Arts (**DSITIA**)
- Department of Transport and Main Roads (**DTMR**); and
- Rockhampton Regional Council (**RRC**).

## 4 Receiving complaints

---

### **Privacy requirements**

#### **IPP1 - Collection of personal information (equates to NPP1)**

IPP1 requires that when agencies collect personal information:

- the personal information is collected for a lawful purpose directly related to a function or activity of the agency
- the personal information is necessary for the fulfilment of that purpose; and
- the collection is not unfair or unlawful.

Complaint handling is an agency function that is common to all government agencies. It is a key feature of an accountable and open government and is an important part of customer service. For local government, this function is in part, defined in legislation.<sup>14</sup>

To avoid any question arising about whether or not an agency is collecting irrelevant personal information, the agency's processes should give careful consideration as to whether each piece of information is in fact necessary in order for it to handle the complaint. If the information is not necessary, it should not be collected.

#### **IPP2 - Collection of personal information (equates to NPP1)**

IPP2 requires that when an agency collects personal information from the individual, the agency takes reasonable steps to make the individual generally aware of:

- the purpose for the collection
- any lawful authority or requirement for the collection
- the identity of the entity the agency may pass the information onto; and
- as appropriate, the identity of a second entity the information may be passed onto.

---

<sup>14</sup> Section 306 of the *Local Government Regulation 2012* and section 279 of the *City of Brisbane Regulation 2012*.

## **Privacy requirements**

### **IPP2 - Collection of personal information (equates to NPP1)**

OIC's term for this information is a 'collection notice'. A collection notice for complaints handling could be included on the agency's complaints web page or form, provided verbally from a script when a complaint is made by the telephone or face-to-face and included in any pamphlets or brochures that the agency makes available about their complaints handling process.

### **IPP3 - Collection of personal information (equates to NPP3)**

Both IPP1 and IPP3 require that when an agency collects personal information it must be directly related to a function of the agency and relevant to fulfilling that function.

If, for example, an agency collects a complainant's date of birth, it must be able to show that it is necessary to collect this information to enable it to deal with the complaint.<sup>15</sup> A clear distinction should be made about the information which is mandatory for the complaint process and the information which is optional. If for example, the complaint form collected demographic information from the complainant for identifying opportunities for service improvement, the collection notice should make the individual aware of this additional purpose and clearly indicate that provision of this information is optional.

IPP3 also requires that an agency take all reasonable steps to ensure that the way that personal information collected from an individual who is the subject of the information does not unreasonably intrude into the personal affairs of the individual. One way of incorporating this requirement is to ask the complainant how they would like to be contacted.

---

<sup>15</sup> This would not necessarily be difficult to identify. If, for example, the complaint concerned denial of a service due to age restrictions, the age of the complainant would be relevant in determining whether this was a valid reason for the denial.

### **Key findings**

- In many cases agencies have published a complaints management policy and procedures on the agency website that include an explicit statement that information will be handled in accordance with the IP Act.
- Some agencies provided detailed information on how personal information would potentially be dealt with in the course of handling a complaint.
- Agencies provided clear advice about the types of complaints that could be dealt with by the agency.
- Complaint forms were designed to minimise the collection of unnecessary and irrelevant information.
- Agencies provided the option for an individual to lodge an anonymous complaint where appropriate.
- Agencies used complaint forms, web pages and scripts for use by call centre or counter staff to communicate collection notices.
- Agencies clearly distinguished between information that was mandatory for a complaint and information that was optional for the complaint.
- In order to maximise compliance with the IPPs, reasonable steps were taken by some agencies to ensure that an individual was generally made aware of the differing purposes for which complaints information was used and what information was used for which purpose.
- Agency complaint forms provided the option for the complainant to nominate their preferred method of contact.

#### **4.1 Fair collection and handling of personal information**

The desktop review found that the majority of agencies published a complaints management policy on their website and that most policies included explicit mention of privacy. Typical policy statements are included in the following table.

### **Examples of reviewed agencies' privacy-appropriate policy statements**

- *Personal information obtained through and in connection with complaints will be collected and handled in accordance with the 11 information privacy principles in the Information Privacy Act 2009 (Qld).*
- *Personal information collected from all parties involved in the complaint process will be handled in accordance with the Information Privacy Act 2009 (Qld).*
- *Personal information is managed in line with the Information Privacy Act 2009 (Qld).*

OIC noted that a number of complaints management policies stated that complaints would be handled in a confidential manner. Confidentiality is a concept that is related to, but different from privacy. Confidentiality is about limiting the disclosure of information, usually through agreement or operation of law, and can be applied to information other than personal information. Privacy relates to the right of an individual to expect agencies to meet their privacy obligations and to protect the personal information of individuals.

In order to deal effectively with a complaint, it may be necessary for an individual's personal information to be provided to other parties regardless of the wishes of that individual. The limits of confidentiality should be explained to the parties to a complaint as part of the information provided about the complaint process.

Even though an agency may take steps not to disclose the name of a complainant, the circumstances may be such that an individual's identity is 'reasonably ascertainable' from the subject of the complaint itself. In general, the IP Act requires that personal information may not be disclosed to a third party<sup>16</sup> unless an exemption applies.<sup>17</sup> These exemptions include where the individual, the subject of the personal information, is reasonably likely to be aware that it is the agency's usual practice to disclose their personal information<sup>18</sup> or where the disclosure of personal information is 'authorised or required by law'.<sup>19</sup>

<sup>16</sup> Outside the agency; information can flow within an agency to enable it to deal properly with the issue the information concerns.

<sup>17</sup> There are six exemptions in both IPP11 and NPP2.

<sup>18</sup> IPP11(1)(a).

<sup>19</sup> IPP11(1)(d) and NPP2(1)(f) provides that disclosure of personal information could occur where the disclosure is authorised or required under a law, such as the common law obligation to satisfy natural justice or the provisions in *Local Government Regulation 2012* (Qld).

Some agencies provided detailed information on how personal information was likely to be dealt with in the course of handling a complaint, either in their complaints management policy and procedures, or in a fact sheet available for download from the agency's website. This approach informed individuals involved in the complaint, at the outset, how their personal information could be used and disclosed, so that the individuals can take this into account when communicating with others during the complaint handling process.

The table below provides examples of notifications OIC considers are effective in communicating to potential complainants about the use and disclosure of personal information collected when handling a complaint.

**Example of effective notification – Example A**

*Complaints will be dealt with in a confidential manner that is respectful to both the complainant and the respondent. Reasonable steps will be taken to protect personal information from loss, unauthorised access, use, disclosure or any other misuse during the complaint handling process. However, the department cannot give an assurance of absolute confidentiality, given statutory obligations and principles of natural justice.<sup>20</sup>*

**Example of effective notification – Example B**

*Council officers must consider statutory obligations, including the Local Government Regulation 2012 and the applicability of the privacy principles in the Information Privacy Act 2009 (Qld) when handling complaints.*

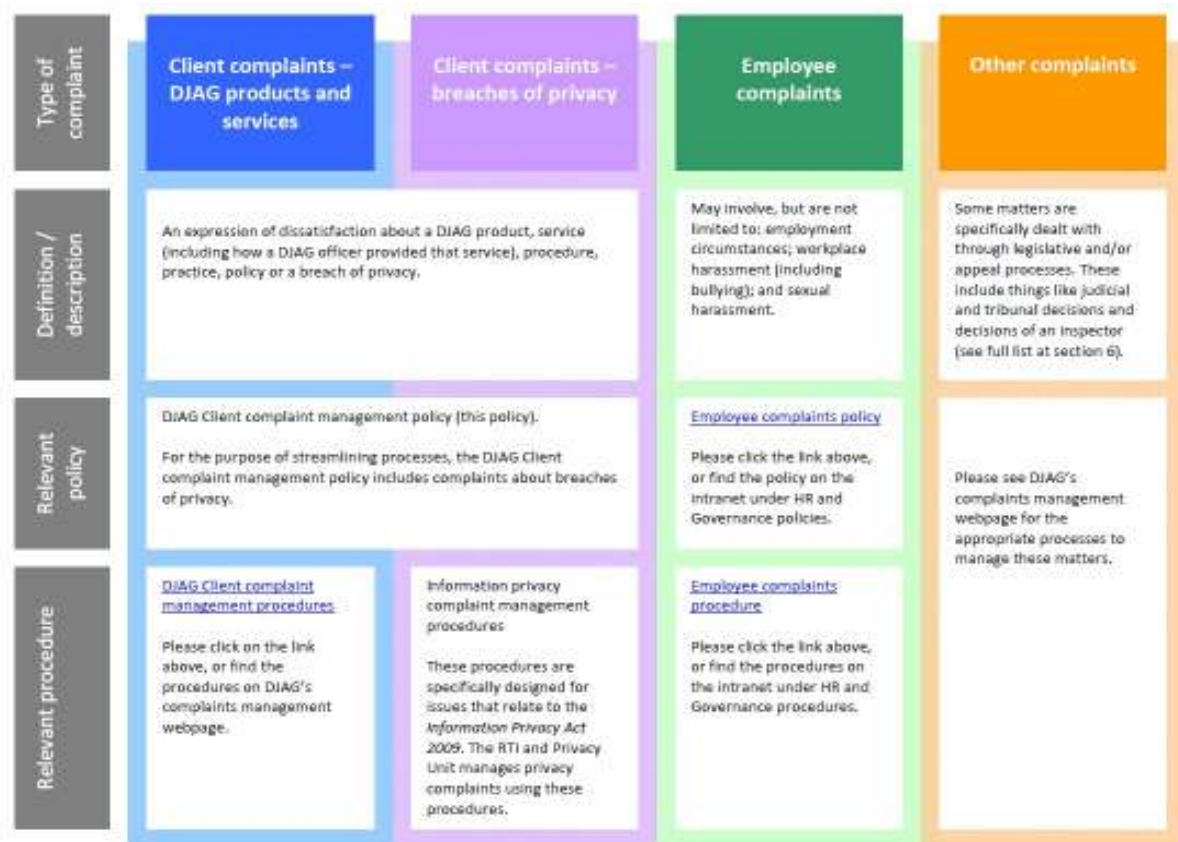
*Complaint handling requires management of personal information, including personal details about complainants, respondents, witnesses and information about the progress and outcome of an investigation.<sup>21</sup>*

<sup>20</sup> Department of Communities, Child Safety and Disability Services – Complaints Management Policy, viewed at <http://www.communities.qld.gov.au/resources/corporate/complaints/complaints-management-policy.pdf>, November 2013.

<sup>21</sup> City of Gold Coast – Complaints (Administrative Actions) Policy, viewed November 2013 and available at [http://www.goldcoast.qld.gov.au/documents/bf/Complaints\\_\(Administrative\\_Actions\)\\_Policy\\_Publications\\_Scheme.pdf](http://www.goldcoast.qld.gov.au/documents/bf/Complaints_(Administrative_Actions)_Policy_Publications_Scheme.pdf).

The in-depth review found that the process for making and handling a complaint differed across agencies according to the type of complaint; who made the complaint; and whether the matter being complained about was specifically dealt with through legislative and/or appeal processes.

OIC considers the following framework used by DJAG<sup>22</sup> provided clear and effective advice to complainants on the circumstances in which the complaints management policy applied and to whom it applied:



**Figure 1: Complaints management framework**

The above framework was supplemented with links to further information about those complaints with different management processes (for example, complaints about a licensing decision), making it easy for a member of the public to find where these types of complaints should be directed.<sup>23</sup>

<sup>22</sup> DJAG Client complaint management policy, viewed November 2013 at [http://www.justice.qld.gov.au/\\_data/assets/pdf\\_file/0004/26266/client-complaint-management-policy.pdf](http://www.justice.qld.gov.au/_data/assets/pdf_file/0004/26266/client-complaint-management-policy.pdf).

<sup>23</sup> See <http://www.justice.qld.gov.au/corporate/contact-us/compliments-and-complaints> for more information.



A hallmark of a good complaints management system is that members of the public can easily find out where and how to complain.

All the agencies selected for in-depth review advised that where a complaint was related to the functions of another agency, they would check with the complainant before referring the complaint to that agency. The IP Act allows the disclosure of personal information where an individual has expressly (or impliedly) agreed to the disclosure. If there is ever any question as to whether or not an individual has impliedly agreed to disclosure, there is an objective test that is applied.

#### **Written procedure for handling referral of complaints**

DTMR's *Complaint Management Procedures*<sup>24</sup> included formal guidance for employees on how external referrals were to be managed:

*Complaints about another agency or organisation are referred immediately, if the complainant has provided consent for their personal details to be released. If consent is not provided, advise the complainant to lodge their complaint directly with the agency or organisation and if possible, provide them with the relevant contact details.*

A copy of DTMR's *Transfer of Information between Queensland Government Agencies* fact sheet is provided in Appendix 3 and provides further guidance and examples of where an agency could reasonably refer correspondence for response by another organisation without consent. Appendix 3 also provides examples of when not to refer correspondence without consent and examples of notifications that should be sent when a complaint is referred.

As complaints can often include sensitive personal information, requesting express agreement before referring a complaint is good practice.

## **4.2 Complaint forms**

Complaint handling invariably involves collecting personal information from various sources. These may include the individual who made the complaint, any individual who is the subject of the complaint, any third parties to the complaint such as witnesses, or any

<sup>24</sup> DTMR *Complaints Management Procedures*, viewed at <http://www.tmr.qld.gov.au/~media/aboutus/contactus/complaintsmanproceduresaug13.pdf>, November 2013.

other persons who may be able to provide information relevant to the complaint – such as specialist experts.

Using a form to collect information from a complainant can be an effective way of controlling the information the agency obtains from the complainant. This ensures agencies receive only necessary or relevant information.

A form that clearly indicates which information fields are mandatory and which are optional can provide a measure of assurance to the complainant that the agency is primarily collecting information of direct relevance to the complaint. It also allows the complainant some control over the information that will be dealt with in the complaint and by implication provides some protection of their privacy.

The review found that agencies offered a range of methods for making a complaint, with nearly half of all reviewed agencies providing an online or downloadable complaint form (or both) for individuals to use when making a complaint.

In some instances, agencies had only a single complaint form for individuals to make any type of complaint. Other agencies provided multiple complaint forms, such as one form for general complaints and another form for specific areas of complaints – for example, breaches of privacy.

An effective approach used by DJAG was to provide a complaint form that required the complainant to tick a box as to the subject matter of the complaint. Having the one multi-function form meant the complainant did not have to search for ‘the correct complaint form’. It also meant that the agency had an easy indicator of the type of complaint being made. In turn this provided for quicker referral to the business area in the agency with responsibility and expertise in responding to complaints about the identified subject matter. A copy of this complaint form is provided in Appendix 4.

The DJAG form also allowed complainants to specify their preferred method of contact.

A review of complaint forms in those agencies selected for in-depth review found that in addition to publicly-available complaint forms, some agencies had formal mechanisms in place to handle verbal complaints, such as using complaint intake forms or customer relationship management systems to record the complaint. This approach was taken to ensure that consistent information was collected from complainants and to assist staff in meeting their obligations when collecting personal information directly from the individual. An example of a complaint intake form used by DSITIA is provided in Appendix 5.

The review also found some agencies used fact sheets, brochures and a complaints web page to assist complainants as to how to make a complaint, what information to include with the complaint and provided privacy-related advice, such as what the information would be used for, who it would be disclosed to and how the information would be stored.

### **4.3 Collection notices**

IPP2 requires that an agency takes reasonable steps to ensure that an individual is made aware of why their personal information is being collected and to whom this information is usually disclosed.<sup>25</sup> [OIC uses the term 'collection notice' to refer to this bundle of information.]

Even though in the case of a complaint made anonymously the agency would not be required to provide a collection notice in accordance with IPP2, it may still be useful. Advice on how the information in the complaint would be used and potentially disclosed to others could be provided in the interests of promoting the agency's open and transparent complaint process.

The review found agencies met their obligation to let individuals know why their information is being collected and how it would be used and disclosed by:

- the inclusion of collection notices in agency complaint forms
- providing scripts for call centre or counter staff to read from when receiving a verbal complaint
- using agency web pages to provide collection notices; and
- incorporating these collection notices in fact sheets dealing with making complaints to the agency.

It is common practice for agencies across the sector to use collection notices to comply with their obligations under IPP2. The collection notice is usually given at the time the personal information is collected. This review found the agencies reviewed in-depth used the collection notice as an opportunity to provide additional information on the potential information flows from the complaint process. This enabled a complainant to make a more informed decision about whether to proceed with their complaint.

---

<sup>25</sup> Under IPP2 and NPP1, an agency is required to take reasonable steps to ensure that an individual is aware of the purposes for which their personal information is being collected, any law that requires the particular information to be collected and the entities to which the agency usually discloses information of that kind.

An example of a 'fuller' collection notice was the one used by DJAG within its online and downloadable complaint forms.

#### **Example collection notice**

*The Department of Justice and Attorney-General (DJAG) is collecting your personal information for the purposes of identifying and dealing with your complaint, in accordance with the Department's Client Complaint Management Policy. Your personal information may be forwarded to the business unit or region relevant to your complaint so your complaint can be addressed. Your personal information will not be provided to any person you are complaining about, unless it is specifically required to ensure your complaint is appropriately dealt with. Any use of your personal information will be limited to that necessary to investigate and respond to the issues raised in your complaint.<sup>26</sup>*

Similarly, the City of Gold Coast provided a collection notice on their *Complaint Lodgement Form*, which usefully included information specific to local governments.

#### **Example collection notice**

*Gold Coast City Council collects personal information in accordance with the Local Government Act 2009 in order to investigate complaints. The information will be used only by authorised officers and, in the case of escalated complaints, by authorised State government agencies for the purpose of reviewing decisions. Please be aware that while the identity of a complaint will not be disclosed, in certain circumstances, the subject of the complaint, of itself, will identify a complainant, e.g. a dividing fence. Information collected may be used to ensure Council's records are accurate. Details of complaints are stored on a secure file and only de-identified information is used for reporting purposes. Your information will not be given to any other person or agency unless you have given us permission or we are required or allowed to by law.<sup>27</sup>*

The collection notice provided to individuals who make a verbal complaint can be the same as, or equivalent to, the collection notice included on the complaint form.

<sup>26</sup> DJAG Complaint form, viewed at [http://www.justice.qld.gov.au/data/assets/pdf\\_file/0018/207252/complaint-form.pdf](http://www.justice.qld.gov.au/data/assets/pdf_file/0018/207252/complaint-form.pdf), November 2013.

<sup>27</sup> City of Gold Coast Complaint Lodgement Form, viewed at [http://www.goldcoast.qld.gov.au/documents/fa/general\\_complaints.pdf](http://www.goldcoast.qld.gov.au/documents/fa/general_complaints.pdf), February 2014.

For example, DTMR's *Complaints Management Procedures* contained an approved collection notice for use when receiving a complaint, as shown below, and required that the collection notice was read out when taking a verbal complaint.

**Approved collection notice:**

*The Department of Transport and Main Roads is collecting your personal details for the purpose of responding to your feedback. Your information will not be disclosed to a third party without your consent unless required or authorised to do so by law.*

**Collection notice read to complainants - Request for consent:**

*If necessary, do you give consent for your personal details to be provided to a relevant third party external to the department for the purpose of finalising your feedback.*<sup>28</sup>

Similarly, DSITIA's *Complaints management procedure* stated complaints received verbally would be treated as if received in writing and that complainants must be provided with the following privacy notice.

**Privacy notice**

*The department is collecting your personal information for the purpose of assessing and resolving your complaint. Your personal information will be disclosed within the department only as necessary for the management of your complaint. Your personal details will not be disclosed to any other third party or used for any other purpose without your consent, unless authorised or required by law.*<sup>29</sup>

In general, the IP Act requires that personal information may not be disclosed to a third party<sup>30</sup> unless an exemption applies.<sup>31</sup>

If an agency will be relying on the exemption that an individual is reasonably likely to have been made aware that it is the agency's usual practice to disclose that type of personal information to a third party, it may be beneficial to have evidence that a collection notice was provided. Even though IPP2 does not require confirmation that the collection notice has been understood (or indeed – even read) an agency can optionally seek assurance


<sup>28</sup> DTMR *Complaints Management Procedures*, viewed at <http://www.tmr.qld.gov.au/~media/aboutus/contactus/complaintsmanproceduresaug13.pdf>, November 2013.

<sup>29</sup> DSITIA *Complaints management procedure*, viewed at <http://www.qld.gov.au/dsitia/assets/documents/complaints-management-procedure.pdf>, November 2013.

<sup>30</sup> Outside the agency; information can flow within an agency to enable it to deal properly with the issue the information concerns.

<sup>31</sup> There are six exemptions in both IPP11 and NPP2.

that the content of the collection notice has been relayed to its intended recipient. One agency reviewed in-depth had adopted this practice. Section 5.1 provides an example of a complaints register that records delivery of a collection notice.



The review identified that further guidance is needed on **collection, storage and security of personal information in complaints**. OIC will develop resources to provide specific advice about how the privacy principles can be incorporated into a Complaints Management Policy and Procedure, including complaints forms.

#### 4.4 Allowing complaints to be made anonymously

Just over half of the agencies reviewed stated in their complaint handling policies or procedures that complaints could be made anonymously. A small number of agencies explicitly stated that complaints could not be made anonymously.

The extent to which it is 'necessary' to require a complainant to provide identifying information will vary according to the type of complaint. For example, if a person complains about a matter that does not personally link them to the subject matter of the complaint (for example, 'complaints' about a broken public facility, such as a street light or bus shelter), it may not be necessary to collect the personal details of the complainant in order to investigate and address the matter.<sup>32</sup>

Similarly, a date of birth may be relevant in a complaint where confirmation of identity is required to identify the relevant client file held by the agency, such as a complaint about a health service. However, if date of birth has no relevance to the subject matter of the complaint (for example, a complaint is about the cost of a product provided by an agency, or a complaint about a broken link on the agency's website), then the complainant's date of birth should not be collected.<sup>33</sup>

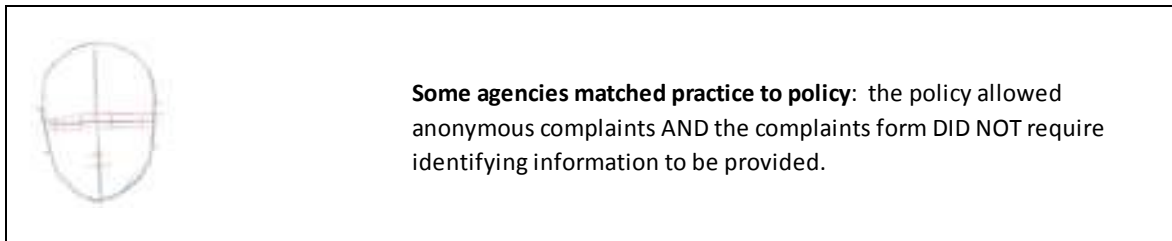
<sup>32</sup> IPP1 obligates agencies to only collect relevant information relating to the agency's stated function and not collect more information than is necessary. If the identity of the complainant is irrelevant to the subject matter of the complaint, then it could be a breach of IPP1 to require the complainant to identify themselves.

<sup>33</sup> Agencies may wish to consider whether or not collection of the complainant's date of birth is necessary if they are not collecting the dates of birth of individuals who are the subject of complaints and nor are they for witnesses or other relevant third parties.

It is not enough for agencies to write a policy allowing for anonymous complaints: agencies should also ensure that agency practice supports the making of anonymous complaints.

The desktop review identified agencies with complaints handling policies or complaints pages that explicitly allowed anonymous complaints, which also had structured complaints forms for the submission of complaints. The desktop review examined whether or not agency policy for anonymity was supported by agency practice in the collection of information on the structured complaint form.





Some agencies matched practice to policy: anonymous complaints were allowed in the agency's policy and the structured complaint form supported the making of anonymous complaints.



**Figure 2: Agencies matching practice to policy.**

Some agencies did not match practice to policy: the agencies had a policy allowing anonymous complaints and the complaints form required one or more types of identifying information. For example, the review found that agencies that allowed anonymous complaints sometimes used a complaint form that required complainants to provide their name or to provide multiple types of information that might enable the complainant to be identified.

Figure 3 depicts the different types of inconsistency between policy and practice for making anonymous complaints that were found in the desktop review.

Identifying information required by some agencies with policies allowing anonymous complaints	
	Required information that the agency could use to investigate and discover the complainant's identity, e.g., the complainant was required to advise the agency whether or not he or she had previously contacted the agency on the same issue.
	Required information that could reveal the complainant's identity, e.g., the complainant was required to provide their email address, which might have contained the complainant's name within the address.
	Sometimes required the complainant's name as mandatory.
	Always required the complainant's name as mandatory.

**Figure 3: Consistency between policy and practice for making an anonymous complaint<sup>34</sup>**

It is good practice for agencies to ensure that policy and practice align, that anonymous complaints should be considered for inclusion in an agency's complaint handling policy and that policy should be carried through to practice.

All six agencies selected for in-depth review allowed complaints to be made anonymously. It was commonly stated that the major challenge in handling anonymous complaints was the agency's inability to contact the complainant to obtain additional information where further information was required to investigate the complaint, but that all reasonable action would be taken to investigate the complaint using the information as provided by the complainant.

The below example demonstrate how these agencies have addressed handling of anonymous complaints in their complaints management procedures.

<sup>34</sup> Images for the diagram on anonymity were provided by wikiHow, a wiki aiming to build the world's largest, highest quality how-to manual. Please view this image in the editable article here <http://www.wikihow.com/Draw-a-Face> and find author credits at wikiHow.com. Content on wikiHow can be shared under a Creative Commons License with attribution to the original author, Ben Rubenstein, Alex, Flickety, Glutted and others.



### Written procedure for handling anonymous complaints - Example A

*Where sufficient information is provided to allow an investigation, anonymous complaints are to be handled in the same manner as all other complaints with the obvious exception of advising of the outcome to the complainant.*<sup>35</sup>

### Written procedure for handling anonymous complaints - Example B

*Anonymous complaints are received verbally and in writing. They're accepted and treated like any other complaint, however the quality and quantity of information provided may restrict how they're investigated.*

*With a verbal complaint, advise the complainant that sufficient detail is required to enable an investigation. Obtain all reasonable information and if possible, provide a reference number to enable the complainant to follow up on progress or to provide further information.*

*Anonymous complaints lodged via our website online form are provided with a contact confirmation number.*<sup>36</sup>



The review identified that guidance is needed on **anonymity, confidentiality and privacy in complaints**. OIC will develop resources to provide further information on:

- how to identify information not necessary to action the complaint
- identifying information that is optional for the complaint; and
- identifying information required for the complaint.

## 4.5 Limiting the collection of personal information to relevant information

The review of complaint forms found that information being collected from complainants included information about the person's gender, age, indigenous status, disability status and cultural background.

<sup>35</sup> City of Gold Coast – *Complaints (Administrative Actions) Policy*, viewed at [http://www.goldcoast.qld.gov.au/documents/bf/Complaints\\_\(Administrative\\_Actions\)\\_Policy\\_Publications\\_Scheme.pdf](http://www.goldcoast.qld.gov.au/documents/bf/Complaints_(Administrative_Actions)_Policy_Publications_Scheme.pdf), February 2014.

<sup>36</sup> DTMR *Complaints Management Procedures*, viewed at <http://www.tmr.qld.gov.au/~media/aboutus/contactus/complaintsmanproceduresaug13.pdf>, November 2013.

In some instances, information was being collected to determine whether the complainant had any accessibility needs. However, agencies should apply caution in wording this question to avoid collecting any irrelevant personal information. Consider the following examples:

**Example**

- ✗ Do you have a disability or other special needs?
- ✓ Do you have a disability or other special needs that would need to be taken into account when we deal with your complaint or when we communicate with you?

Demographic information about complainants is commonly collected to provide information that can be used to assess the differing service delivery needs for people from a range of backgrounds. However people sometimes consider demographic questions to be highly personal and/or intrusive<sup>37</sup> and there is the potential for this to affect the way they engage with the agency.<sup>38</sup> An agency needs to give careful consideration to the purpose for which the demographic information will be used and to collect only personal information necessary for the intended use.<sup>39</sup>

The purpose of collecting demographic information is secondary to the purpose of assessing and actioning a complaint. Where personal information is collected for more than one purpose, it is important that an individual is made aware of the multiple purposes and can identify what information will be used for which purpose.

Although the provision of the demographic information should be optional, the individual should also be assured that their non-provision of demographic information will have no adverse impact on the primary purpose for the information collected in the form – the management of their complaint.

<sup>37</sup> In the NPPs, demographic information is classed as 'sensitive information' and warrants additional protections.

<sup>38</sup> For example, by providing false information.

<sup>39</sup> Collecting personal information because the agency thinks it may be useful at some time in the future is a potential breach of IPP1 and NPP1.



The [OIC Guideline: Demographics and privacy](http://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/demographics-and-privacy)<sup>40</sup> provides further information on the collection of demographic data, its potential impact on an individual's privacy and examples of collection notices that cover multiple purposes.

## 4.6 Training and awareness

All employees have the potential to be involved in complaint handling. Good privacy practice requires that agencies provide training and/or information to all their employees about the agencies' complaint handling policies. Preferably, this would be communicated to employees when they first start work for the agency as part of the agencies' induction packages, and at regular intervals for existing employees. The training would cover the agency's complaints management policy, with additional, detailed training and resources being provided for those staff involved in receiving and investigating complaints.

For example, DTMR's *Complaints Management Procedures* showed a strong commitment to training and awareness:

### ***Complaints management training***

*To raise staff awareness and understanding of responsibilities, we provide training and promote complaints management through:*

- *activities, such as departmental messages, posters and screen savers*
- *induction programs and information awareness sessions*
- *training materials and resources, such as FAQs, how-to guides and examples*
- *the online Managing Complaints and Investigating Complaints courses*
- *face to face training sessions or personal coaching*
- *the departmental champion and Branch Complaints Coordinator Network.*

<sup>40</sup> This link can be accessed at <http://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/demographics-and-privacy>

### **Complaints management training**

*All staff with complaint management responsibilities are encouraged to complete the Managing Complaints and Investigating Complaints online courses. Directors also ensure these staff have access to appropriate information and training within their branch. Staff members nominated as an authorised officer are required to successfully complete the online Managing Complaints course.*<sup>41</sup>

As part of OIC's role in promoting the principles and practices of information privacy, the OIC provides a range of professional development training courses to support agency practice in information privacy.



The OIC's [Privacy Complaint Management online training](http://www.oicqld.e3learning.com.au/content/signup/information.jsp)<sup>42</sup> provides training in the identification and management of complaints about breaches of the *Information Privacy Act 2009* (Qld). The course provides information about what constitutes a privacy complaint and the key factors in successfully resolving a privacy complaint.

<sup>41</sup> DTMR *Complaints Management Procedures*, viewed at <http://www.tmr.qld.gov.au/~media/aboutus/contactus/complaintsmanproceduresaug13.pdf>, November 2013.

<sup>42</sup> This link can be accessed at <http://oicqld.e3learning.com.au/content/signup/information.jsp>

## 5 Recording complaints

---

### **Privacy requirements**

#### **IPP4 – Storage and security of personal information (equates to NPP4)**

Once an agency has collected information about a complaint, IPP4 requires that the agency must ensure that personal information is protected against loss, unauthorised access, use, modification, disclosure or any other misuse. This is an absolute obligation; there is no 'reasonableness defence'.

Common situations that could result in a privacy breach include:

- unauthorised access or misuse of complaint records by a staff member
- failure to store complaint records containing personal information appropriately or dispose of them securely
- loss or theft of documents, computer equipment or portable storage devices containing complaint records
- mistaken release of records to someone other than the intended recipient; and
- unauthorised access of databases by someone outside the agency.

Security requirements differ depending on the type and amount of personal information held by the agency. The whole-of-government Information Standard 18 applies to departments and some other agencies, and provides general guidance to all agencies in this area. Security measures can include:

- Physical – locks and swipe cards to control access to restricted areas, provision of confidential destruction bins
- Electronic – group permissions to control access to shared directories, information classification labels to control access to records in information systems, secure portable data storage devices such as encrypted flash drives when taking data offsite; and
- Operational – training in security awareness, 'clean desk' policy.

## **Privacy requirements (cont.)**

### **IPP8 – Checking of accuracy etc. of personal information before use by agency (equates to NPP3)**

IPP8 requires that an agency takes all reasonable steps to ensure that information is accurate, up to date and complete before using the information for its specified purpose. In addition, all Queensland public sector employees have a responsibility under the *Public Records Act 2002* (Qld) to keep full and accurate records of their business activities.

### **Key findings**

- Standardised or centralised complaints registers were an effective way to control what information was recorded about complaints for the purposes of tracking, monitoring and potential use by external review bodies.
- Some agencies provided useful recordkeeping guidance on what information and evidence was required to make a complaint file a full and accurate record.
- While agencies had implemented sound data security practices for information obtained in the course of their CMS, they had limited formal documented guidance for these security measures.
- A robust security measure for complaints documents adopted by some agencies was to have processes that ensured that employees accessed only those records necessary for them to complete their business role.
- Access to complaints records was determined by the relevance of the records to the performance of their duties and their level of delegated authority.
- Some agencies took the opportunity of the provision of a collection notice to provide complainants with information on their security of complaint documentation.

## 5.1 Registering complaints

It is a common feature of a CMS that there are mechanisms in place to gather and record information to:

- meet any statutory, policy or procedural reporting requirements
- identify complaint trends; and
- monitor the time taken to resolve complaints.<sup>43</sup>

The in-depth review found that a number of agencies usefully set out requirements for maintaining a complaints register in their complaints management procedures. For example, City of Gold Coast provides the following advice in their *Complaints (Administrative Actions) Policy*:

### **Complaints Register**

*Every complaint received by Council that is within the scope of the Complaints (Administrative Actions) Policy, regardless of how quickly it is resolved, must be entered into the directorate/branch Complaints Register by either the person taking the initial call, or the people investigating the complaint (i.e. either the original decision maker, or the Complaints Officer) to allow tracking, monitoring and reporting. The Register forms the basis for Council's review and reporting of its complaints management process and its outcomes including improvements to business practices and policies.*

*The Complaints Register includes provision to record any identified system problems of business improvements resulting from investigation of complaints including new or revised processes, practices and policies. The officer investigating the complaint must also report such problems and improvements to the relevant Manager who is responsible for implementing change and reporting.*

*The Complaints Register details the way in which complaints are to be classified to assist in meaningful analysis and reporting.*<sup>44</sup>

<sup>43</sup> Queensland Ombudsman's *Effective Complaints Management Fact Sheet: Monitoring Effectiveness*, viewable at <http://www.ombudsman.qld.gov.au/Publicagencies/Resources/EffectiveComplaintsManagement/ComplaintsManagementResources/EffectiveComplaintsManagementFactSheets/tabid/148/Default.aspx>.

<sup>44</sup> City of Gold Coast – *Complaints (Administrative Actions) Policy*, viewed November 2013, viewable at [http://www.goldcoast.qld.gov.au/documents/bf/Complaints\\_\(Adminstrative\\_Actions\)\\_Policy\\_Publications\\_Scheme.pdf](http://www.goldcoast.qld.gov.au/documents/bf/Complaints_(Adminstrative_Actions)_Policy_Publications_Scheme.pdf).

CQUniversity provided a centralised Customer Relationships Management system for students to log compliments, provide feedback, and make complaints about any aspect of University life.

Another effective approach was taken by DSITIA, who used the complaints register to record whether a collection notice was delivered and to provide the following step by step directions:

### **Complaints Register**

*To assist the department in monitoring effectiveness of the complaints management system, all complaints must be recorded in an electronic complaints register by departmental employees or local managers.*

*The electronic complaints register must include the following details as a minimum:*

- *a sequential complaint number*
- *date complaint received*
- *name of departmental employee to whom complaint was made*
- *service/departmental employee area location*
- *mode of complaint (e.g. email, letter, telephone, etc.)*
- *complaint level (e.g. 1, 2 or 3)*
- *privacy notice given (e.g. Y/N)*
- *nature of complaint (e.g. service/product or employee)*
- *name of departmental employee dealing with the complaint*
- *outcome/resolution*
- *action taken by department*
- *date complainant notified*
- *method used to communicate outcome to the complainant*
- *business improvement required (e.g. Y/N)*
- *response time (business days)*
- *complaints of a similar nature (e.g. Y/N).*<sup>45</sup>

An example of the complaints register used by DSITIA is provided in Appendix 6.

<sup>45</sup> DSITIA *Complaints management procedure*, viewed at <http://www.qld.gov.au/dsitia/assets/documents/complaints-management-procedure.pdf>, November 2013.



## 5.2 Recordkeeping requirements

Good recordkeeping practices are a key factor in an agency meeting the obligations in the IP Act to take reasonable steps to ensure that personal information is accurate, complete and up to date before it is used.

The review found that each of the agencies selected for in-depth review included in its complaints management policies and procedures an explicit commitment to creating complete and accurate records of all material relating to a complaint. Examples of two good features of complaints documentation are provided below.

Some policies and procedures advised that access to complaints information or documents was subject to the provisions of the RTI Act or IP Act. For example, DJAG's *Client complaint management handbook* stated:

### **Recordkeeping requirements**

*Complaint officers are responsible for ensuring the complete and accurate recording of all material relating to a complaint (including actions and decisions made regarding issues resolved at the frontline) as required by section 7 of the Public Records Act 2002.*

*Each complaint file must contain all correspondence, file notes of any telephone conversations, interviews and findings from investigations, recommendations and internal approvals. The file must also contain an explanation for the actions taken in investigating a complaint. The file will be available for internal and external review, subject to privacy and right to information considerations.<sup>46</sup>*

---

<sup>46</sup> DJAG *Client complaint management handbook*, viewed December 2013.

DTMR's *Complaints Management Procedures* provided clear direction on what information must be captured on a complaint file:

### **Recording a complaint**

*Recordkeeping is the responsibility of all staff and managed in line with the Public Records Act 2002. Complaint records/ files are retained as per the recordkeeping framework and destroyed under an approved retention and disposal schedule. Records/ files with confidential, sensitive and/ or personal information must be saved within the recordkeeping system with appropriate security classifications and security access controls. External complaint records managed on DocTrak [the Document Management System] are saved by the Executive Services Unit (Human Resources and Governance Branch) within their recordkeeping database.*

### **Complaints records/files**

*Comprehensive complaint records/ files are essential to ensure complaints are appropriately assessed, investigated and resolved. A full record/file may include any incoming documents, completed Complaint Management Form, file notes, investigation notes, system notes and evidence. It should cover all relevant information from when a complaint is received to when it's finalised, including details of:*

- the complainant's relevant personal information and preferred contact method*
- how the complaint was received and any relevant dates*
- the unique reference or number which enables the complaint to be monitored*
- any staff member(s) who received and/ or managed the complaint*
- the assessed classification and any changes*
- the issues and requested outcome or actions*
- any relevant history, context or significant issues*
- the acknowledgement, communications with and response out to the complainant*
- any planning, research, investigation or action taken*
- the outcome, any evidence and reasons for decisions*
- any advice or approvals granted.<sup>47</sup>*

<sup>47</sup> DTMR *Complaints Management Procedures*, viewed at <http://www.tmr.qld.gov.au/~media/aboutus/contactus/complaintsmanproceduresaug13.pdf>, November 2013.

### 5.3 Storage and security of complaint information

The security measures that an agency takes to protect documents containing personal information should be 'adequate to the level of protection that can reasonably be expected to be provided'.<sup>48</sup> Factors agencies may wish to take into consideration in assessing reasonable protection would be the likelihood of a breach occurring and the level of harm that could result from a breach. Some types of personal information may require more stringent protections due to the sensitivity<sup>49</sup> or breadth of the personal information contained in those documents. For example, it may be reasonable to expect that agencies will use stronger measures to protect information relating to employee complaints that include allegations of misconduct by another employee, than they would complaints about an agency's failure to fix a broken street light.

Agencies should refer to *Information Standard 18: Information Security*<sup>50</sup> as a starting point for advice on implementing appropriate security controls to protect the information they hold.

OIC's review found that agencies' complaint handling policies generally included a high level statement about the agency's storage and security of complaint information, with the following statement being typical:

#### **Storage of complaint information**

*Documentation relating to complaints is stored securely. Information relating to complaints is accessible only by those staff members whose duties require them to use the information.*

<sup>48</sup> IPP4(2).

<sup>49</sup> NPP9 sets out the conditions under which health agencies can collect sensitive information. Generally, sensitive information can only be collected with the individual's consent and there are tighter restrictions on how this type of information can be used and disclosed. Sensitive information is defined in schedule 5 of the IP Act and includes health information, criminal record and information relating to race or ethnic origin, political or religious beliefs, trade union membership and sexual preferences. The IPPs do not refer to sensitive information and agencies are required to handle all information, including sensitive information, in accordance with the IPPs.

<sup>50</sup> Viewable at <http://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2704-information-security-is18>

Agencies had limited formal documented guidance outlining specific security measures for information collected and stored as part of a CMS. OIC's discussions with the agencies selected for in-depth review found that security measures to mitigate security risks included:

- Physical measures:
  - Use of lockable filing cabinets to store hard copy documents
  - Use of confidential destruction bins and shredders
  - Securing premises through locks on doors and swipe cards; and
  - Issuing visitor passes and escorting visitors into and out of secured areas.
- Electronic measures:
  - Storage of complaint files in restricted access folders on shared network drives
  - Assigning classification settings in electronic document and records management systems and other information systems; and
  - Policies and procedures for use of portable storage devices.
- Operational measures:
  - Clean desk policy that specifies how employees should leave their working space when they leave the office
  - Choosing a method of communication that is appropriate for the information being sent (such as registered post)
  - De-identifying complaints information where access to identifying details is not required for the person to carry out their role (for example, when reviewing and reporting on performance measures); and
  - Use of interview rooms for discussions with complainants or third parties to a complaint.

OIC acknowledges an agency's information security policy and recordkeeping policy typically provide direction on the security measures that need to be taken to protect information held by the agency. It can be helpful to include similar advice in the agency's complaints management procedure. For example, an agency could provide practical

advice on managing the security risks that regularly arise when handling complaints as part of the guidance included in the agency's complaints management procedure, or include reference to where this guidance can be found.



The review identified that guidance is needed on **collection, storage and security of personal information in complaints**. OIC will develop resources to provide further information on security considerations that can arise during the handling of a complaint.

#### 5.4 Acknowledging receipt of a complaint

Good communication when managing a complaint will foster confidence in the complaints handling process, which in turn will encourage the cooperation of the parties and a greater acceptance of the outcome.

The in-depth review found that a common key performance measure used by agencies to evaluate handling of complaints was the timeframe for acknowledging receipt of a complaint.

Acknowledging receipt of complaints was used by some agencies as an additional opportunity to deliver a collection notice. While collection notices should be delivered before, or at the same time as, the personal information is collected, providing a collection notice as part of the acknowledgement receipt is a practical way of capturing evidence that a collection notice was delivered. In addition, formally delivering a collection notice is essential if an agency wishes to rely on the exemption in IPP11(1)(a) to defend an individual's assertion they were not 'reasonably likely to have been aware' that an agency usually discloses certain types of personal information as part of the complaint management process.<sup>51</sup>

Acknowledging receipt of complaints was also used by some agencies as an opportunity generally to provide complainants with information about how the agency handles complaints and the agency's policy or framework surrounding the collection, use and disclosure of personal information.

---

<sup>51</sup> IPP11(1)(a).

### **Example of effective acknowledgement – Example A**

When a complaint is lodged online with CQUniversity, students automatically receive an acknowledgement of receipt of their complaint which includes a link to the Student Complaints Policy and Procedures.

### **Example of effective acknowledgement – Example B**

DJAG's *Client complaint management handbook*<sup>52</sup> states that acknowledgement includes:

- *reassuring the complainant that their feedback/complaint is valued*
- *requesting any further information considered necessary to action the complaint*
- *outlining how the complaint will be managed, including a timeframe for resolution*
- *establishing how progress reports will be provided*
- *providing contact details for the complaint officer*
- *advising the complainant about how their personal information will be used.*

An easy way to provide information about how an agency manages, uses and discloses information collected during the handling of a complaint is to incorporate this advice into an information sheet that can then be attached to an acknowledgement letter. A template that could be used by agencies to prepare an information or fact sheet is provided in Appendix 7.

---

<sup>52</sup> Viewed December 2013.

## 6 Processing complaints

---

### **Privacy requirements**

#### **IPP1 to IPP3 – Collection of personal information (equates to NPP1)**

An agency may request personal information from an individual or from a third party provided the following criteria are met:

- the agency must only ask for the specific personal information required to fulfil the lawful purpose that is directly related to the function of the agency
- if the information is collected directly from an individual, the agency must tell the individual what the information is going to be used for before, or at the point of collection where possible; if not possible – as soon as practicable after the information is collected; and
- the agency must not collect information by unlawful or unfair means, including by trickery, deception or misleading conduct.

This obligation extends to witnesses and other third parties who may be interviewed during the investigation of a complaint. Ensuring that these individuals understand the purpose of collecting the information and to whom the information will be disclosed is essential, as is taking steps to make sure that the individual is aware of circumstances when conversations are being digitally recorded.

#### **IPP11 – Limits on disclosure of personal information (equates to NPP2)**

Under IPP11, an agency must not disclose personal information to a third party, unless:

- the individual is reasonably likely to be aware<sup>53</sup> or have been made aware<sup>54</sup> that it is the agency's usual practice to disclose that type of personal information to the third party or
- the individual has expressly or impliedly agreed to the disclosure or
- the disclosure is 'reasonably necessary' to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare or

---

<sup>53</sup> Usually through knowledge of a policy pre-dating July 2009.

<sup>54</sup> Through a collection notice issued in accordance with IPP2.

## **Privacy requirements**

### **IPP11 – Limits on disclosure of personal information (cont.)**

- the disclosure is authorised or required under law or
- the disclosure is ‘reasonably necessary’ for law enforcement purposes; or
- the disclosure is necessary for research or statistical purposes.

Natural justice is a common law obligation for decision makers. As such, disclosing personal information in order to afford someone natural justice falls within the ‘authorised or required by law’ exemption in IPP11(1)(d). The ‘authorisation’ will only apply to the extent that disclosures that are necessary in order to afford procedural fairness. To fall within the permissions and limitations of natural justice, it will only apply to information that is credible, relevant and significant to that complaint.

### **Contracted service providers (Chapter 2, Part 4)**

In the first instance, the privacy principles only apply to Queensland government agencies. They do not nominally apply to private sector firms, community sector organisations or individuals. An exception is where the government agency outsources its functions to a non-government entity and that arrangement involves the flow of personal information. For these arrangements the agency is obligated under Chapter 2, Part 4 of the IP Act to take all reasonable steps to bind the non-government entity to compliance with the obligations under the relevant privacy principles. If so bound, the entity assumes the same obligations as the contracting agency.

The benefit to the agency is that once bound, the entity assumes all liabilities for any subsequent privacy shortfalls.<sup>55</sup> If the agency fails to take all reasonable steps to bind the contractor to compliance with the privacy principles then it retains liability for privacy shortfalls of the contracted entity.

In the complaints process, agencies could contract out the entire complaint management or a part of it. In both cases, agencies should take all reasonable steps to bind the contractor to compliance with the relevant privacy principles.

---

<sup>55</sup> Outsourcing can be a privacy vulnerability for agencies. The *2011 Cost of Data Breach Study: Australia* by the Ponemon Institute found that 36 percent of participating organisations reported that their data breach involved one or more third parties.



## **Key findings**

- Some agencies when entering into contracts or arrangements with external services providers for the investigation of complaints, were taking steps to ensure that the contracted service provider was contractually bound to comply with the privacy principles.
- Agencies policies and procedures focused on meeting their obligation to afford natural justice to a person who was the subject of a complaint.
- More formal guidance was required to make it clear that the obligation to afford natural justice was only required where a decision was going to be made that would adversely affect that person.
- Agencies were providing witnesses and other third parties with a collection notice prior to being interviewed.
- Recording of interviews was transparent with some agencies providing interviewees with a copy of recordings or a written summary for the individual to check that the record of interview was accurate.

## **6.1 Natural justice**

Natural justice provides an individual the opportunity to be made aware of, and respond to information which will be used in the course of a decision, and that might negatively affect that individual.<sup>56</sup> In the context of a complaint made against an individual, natural justice provides them with sufficient information to enable them to understand and respond to the complaint.

Natural justice is an integral part of the processes involving complaints made against individuals. If a complaint is substantiated, any decision made as a consequence will invariably negatively affect the individual who is the subject of the complaint. For example, the outcome of a complaint may be the disciplining of an employee, the imposition of a fine, the negation of a licence or permit or the removal of a benefit, such as a travel concession.

---

<sup>56</sup> See Brennan J, in *Kioa v West* (1985) 159 CLR 550 at 629.

### ***Natural justice and the disclosure of personal information***

The rules governing when an agency can disclose personal information are set out in IPP11. The general rule is that personal information of a person may not be disclosed to a third party. One of the exceptions in IPP11 is where the disclosure of personal information is 'authorised or required by law'.<sup>57</sup>

Natural justice is a common law obligation for decision makers, so disclosing personal information in order to afford someone natural justice falls within the 'authorised or required by law' exception. The 'authorisation' will only apply to disclosures that are necessary to satisfy natural justice in a complaint process. It will only apply to information that is credible, relevant and significant to that complaint and may result in adverse findings against a person.

If an agency discloses personal information outside of the requirements of natural justice, that disclosure can be a breach of the privacy principles and be the impetus for a separate privacy complaint.

While complaint handlers will be very familiar with the permissions and restrictions of natural justice in the complaint process, for the parties in a complaint the concept of natural justice and its application to their circumstances may not be known. Consequently, individuals may be unaware that natural justice will require some information to be provided to other parties. For example, a person who complains that an individual harassed them may not necessarily know that that individual will have to be provided with both their identity and details of the alleged harassment.

Generally, as only individuals who will be negatively affected by a decision are entitled to natural justice, this will only need to be given to the person who is the subject of the complaint. Natural justice would not necessarily require the investigating agency to inform the complainant, witnesses or other people of the full details of the allegation and the outcome or decision reached in relation to the complaint.

IPP2 requires agencies to inform persons from whom personal information is collected why the information is being collected, to whom it would usually be provided and any legislative basis for the collection. The collection notices used in complaints should refer to how natural justice may affect the information flows in the complaint. As with all

---


<sup>57</sup> See for example – section 46(3) of the *Crime and Misconduct Act 2001*.

collection notices, they should be given to the persons involved in the complaint at the commencement of the complaint handling process.

Agencies could also use the opportunity of the provision of the collection notice to inform the parties to a complaint about the information they might expect to receive at the conclusion of the complaint.

The in-depth review found that agencies had a good understanding of when information needed to be disclosed to a complainant to afford natural justice and took steps to disclose only enough information for the individual to understand and respond to the complaint made against them, for example, by summarising the allegation rather than providing unedited copies of documents.

However, all agencies would benefit from clear guidance on the extent of natural justice and how natural justice only applies when an individual will be adversely affected by a decision, and that this rarely applies to the complainant or witnesses.



The review identified that guidance is needed on the **disclosure of personal information and natural justice**. OIC will develop resources to provide further information on the extent to which natural justice applies to the subject of a complaint (the respondent).

## 6.2 Interviewing witnesses and other third parties to a complaint

It is a standard practice for complaint handlers to obtain information relevant to the management of a complaint from interviews with the parties to the complaint. The purpose for interview can range from seeking further information and clarification of the subject matter of the complaint; to obtaining corroborative information from witnesses and other third parties; and to obtaining a response from the individual who is the subject of the complaint.

Interviews are a collection of personal information and accordingly IPP1 to IPP3 apply. If the interviewee will be providing his or her own personal information, IPP2 will apply.

The fundamental principle for the collection of personal information is that the agency should only collect as much personal information as it needs for the management of the complaint. Most interviews will consist of closed questions – requiring a specific answer; and open questions – that the interviewee can respond to as they consider necessary.

For both types of questions care should be taken to focus the interviewee on providing information relevant to the complaint.

In the course of the interview, the interviewer will have to disclose some information to the interviewee in order to elicit the required information. The obligations in IPP11 will apply to these disclosures.

There is the capacity in the IP Act for records of interviews conducted covertly to be not subject to the privacy principles,<sup>58</sup> but generally in a complaint management context, the interviewee will be aware of the fact of the interview. IPP1(2) requires that an agency must not collect personal information in a way that is unfair or unlawful. It is arguable that if personal information is collected from an individual without their being aware of the collection in circumstances where this secrecy is not warranted, the collection is unfair.

The record of interview, whether in the format of interviewer's notes, a written up record of interview or an audio or audio-visual recording, constitutes a document containing the personal information of individuals. While all the IPPs can be applicable to these documents, the IPPs that are of particular importance are IPP4 (the agency's obligation to prevent unauthorised dealings with the document), the access and amendment<sup>59</sup> provisions of IPPs 5-7 and disclosure under IPP11.

In order to comply with these privacy principles, the complaint handler should provide the interviewee with adequate information before the commencement of the interview about the purpose of the interview, their rights of access and amendment of the record of the interview and to whom the record of interview may be disclosed.<sup>60</sup>

The in-depth review found that a good approach taken by agencies was that interviewees were provided with a collection notice in writing prior to the interview being held as part of the confirming the time and date for the interview to occur. Where interviews were recorded, confirmation was again given that the interview was to be recorded. Some agencies advised interviewees that a copy of the recording would be made available to the interviewee if requested, with other agencies providing a written summary of the provided information for the individual to check that the information was accurate.

---

<sup>58</sup> Schedule 1(1)(b) of the IP Act.

<sup>59</sup> Though usually for government agencies, these rights will be more usually exercised under Chapter 3 of the IP Act.

<sup>60</sup> This is in part can overlap with the obligations to provide a collection notice under IPP2 and NPP1(3).

### 6.3 Contracted Service Providers

The in-depth review found that some agencies used external service providers to conduct investigations into some complaints.

Where this occurs, as the agency will be entering into an arrangement with a service provider to perform a function of the agency and will be dealing with personal information for the agency, these arrangements constitute a service arrangement as provided for under section 34 of the IP Act. Accordingly, agencies are required under section 35 to take all reasonable steps to ensure that the contracted service provider is required to comply with the privacy principles. The IP Act describes this process as 'binding a contracted service provider to privacy principles' and describes these service providers as 'bound contracted service providers'.

The contracted service provider should be bound before any personal information held by an agency is provided to them.

The requirement on the service provider to comply with the privacy principles must be clear and specific. Simply stating in the contract or other arrangement that the service provider is to comply with the privacy principles may not be sufficient to satisfy the agency's obligations under section 35 of the IP Act.

Issues that may need to be considered when entering into a service arrangement include:

- transfer of personal information outside of Australia which includes subcontracting overseas, overseas data storage, online transactions including web-sites and social networking use (section 33)
- data breach notification<sup>61</sup>
- privacy complaints handling processes
- lawful use and disclosure and whether the contracted service provider would be required to notify the department if it relies or intends to rely on any of the exceptions in IPP10 and IPP11
- access to and amendment of documents containing personal information (IPP6 and IPP7)
- creation and/or maintenance of a list of personal information holdings

---

<sup>61</sup> Not mandated in the IP Act but desirable from an operational point of view.

- privacy training and awareness for service provider employees; and
- use of sub-contractors.

Examples of such contract provisions used by RRC and the City of Gold Coast to bind contracted service providers are provided in Appendix 8. These examples are of a general nature only and specific facts or circumstances have not been taken into account. The examples should not be relied on as legal advice and OIC suggests that agencies may wish to seek legal advice to determine what requirements to incorporate into formal contract arrangements to bind contracted service providers. However they represent a good guide to the type of contract provisions that could be used.

The in-depth review found that some agencies use a Standing Offer Arrangement to source a service provider. This approach has the benefit that the terms and conditions for the arrangement are applied consistently each time a provider is engaged.



The [OIC Guidelines on Contracted Service Providers](http://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/contracted-service-providers)<sup>62</sup> provide further information on an agency's obligations when entering into contracts or arrangements with another entity to perform one of more services which fall within an agency's functions.

<sup>62</sup> This document can be accessed from this link <http://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/contracted-service-providers>.

## 7 Responding to complaints

---

### **Privacy requirements**

IPP10 (secondary use) and IPP11 (disclosure) (equates to NPP2) provide that personal information will not be used for a secondary use or disclosed to a third party, unless one of a number of exemptions apply.

The exemptions are generally common to IPP10 and IPP11 and include consent by the individual concerned, authorised or required under a law or reasonably necessary for a law enforcement purpose.

'Law enforcement purpose' and 'law enforcement agency' are broadly defined in the IP Act and would cover many complaint processes.

There are also additional limited exceptions under section 29 of the IP Act for law enforcement agencies.

IPP11(1)(a) also allows the disclosure of personal information if the individual concerned is reasonably likely to be aware or has been made aware under IPP2 (through a notice as discussed above) that personal information of that kind is usually passed on to that particular person, body or agency.

### **Key findings**

- Agencies' provide formal guidance on what should be communicated when advising the outcomes of a complaint to parties involved in it, particularly the complainant.

### **7.1 Communicating the outcome of a complaint**

Effective complaints management requires that complainants are provided with timely feedback.<sup>63</sup> However, how much advice or feedback should be given is affected by the operation of the relevant privacy principles.

---

<sup>63</sup> Queensland Ombudsman's *Effective Complaints Management Fact Sheet: Feedback*, viewable at <http://www.ombudsman.qld.gov.au/Publicagencies/Resources/EffectiveComplaintsManagement/ComplaintsManagementResources/EffectiveComplaintsManagementFactSheets/tabid/148/Default.aspx>.

### Example of what should be communicated

DTMR's Complaints Management Procedures<sup>64</sup> provide the following guidance:

Ensure responses are clear, easy to understand and include all relevant details, such as:

- a summary of the complaint and issues
- the process taken, including any actions to resolve the complaint
- the decision and reasons, including an explanation of the remedy
- how and who to contact for future enquiries
- review options if the complainant may be dissatisfied.

Plan a conversation for verbal responses and record full details into an appropriate system or within a file note. Ensure written responses are consistent with the Writing Style Manual and any communication protocols provided by Executive Services Unit (Human Resources and Governance Branch).

All responses should be appropriately approved. In some cases, staff are authorised within their role to respond directly to complaints involving certain issues or are able to use pre-approved response templates or scripts. All other responses should be approved by an authorised officer within the branch.

If insufficient time is taken to explain actions and decisions in a manner that shows the complainant's concerns were properly considered, a minor matter can escalate into a major one.<sup>65</sup> OIC's experience is that a significant proportion of complainants who make a privacy complaint to the Information Commissioner do so because they are dissatisfied with the response provided by the agency in the course of another, earlier complaint. This dissatisfaction is often fuelled by a perceived inadequate explanation by the agency of the outcome of the earlier complaint.

<sup>64</sup> Viewed at <http://www.tmr.qld.gov.au/~media/aboutus/contactus/complaintsmanproceduresaug13.pdf>, November 2013.

<sup>65</sup> Queensland Ombudsman's *Effective Complaints Management Fact Sheet: Communication*, viewable at <http://www.ombudsman.qld.gov.au/Publicagencies/Resources/EffectiveComplaintsManagement/ComplaintsManagementResources/EffectiveComplaintsManagementFactSheets/tabid/148/Default.aspx>.



### Example of how to provide clear reasons

A statement that 'We were unable to uphold your complaint', 'Our actions did not breach the requirements of the IP Act' or 'The conduct by our employees was lawful and appropriate' without supporting evidence and reasoning, is not a reason – it is a conclusion.

A reason addresses:

- *why* you were unable to uphold the complaint
- *why* you were unable to confirm the complainant's version of events
- *why* what was alleged was not improper; or
- *why* you could see no evidence of unfairness, given what the complainant had submitted.<sup>66</sup>

When considering what information to provide to complainants, agencies need to balance:

- the protection of personal information about individuals and the agencies obligations in under the IP Act
- any legislative reporting obligations required of the agency;<sup>67</sup> and
- the need to take reasonable steps to be open, transparent and accountable.

Personal information that needs to be disclosed for one purpose might need protection in other situations. For example, it may be necessary to provide information given by a witness to the person complained about in order to afford the person natural justice. However natural justice rarely applies to the complainant or witnesses, making it unlikely that it is acceptable to disclose this same information when advising the complainant or other people of the details of the outcome or decision reached in relation to the complaint.

## 7.2 How much detail should be given about the outcome or decision?

Agencies can provide general information to complainants about the outcome of investigations. However, just because information might be of interest<sup>68</sup> to a complainant,

<sup>66</sup> Queensland Ombudsman's *Effective Complaints Management Fact Sheet: Feedback*, viewable at <http://www.ombudsman.qld.gov.au/PublicAgencies/Resources/EffectiveComplaintsManagement/ComplaintsManagementResources/EffectiveComplaintsManagementFactSheets/tabid/148/Default.aspx>.

<sup>67</sup> Some legislation sets out what information is obliged to be provided to the complainant eg section 42(7),(8) and section 44(5)(6) of the *Crime and Misconduct Act 2001* (Qld).

this does not necessarily trigger a natural justice obligation to provide them with this information. If communicating the remedy or outcome of a complaint to a complainant involves the personal information of a third party – albeit that party may be the person complained about – this will involve a disclosure of the personal information of the third party.<sup>69</sup> As such, the obligations arising under IPP11 will be applicable.

Disclosure has a specific meaning in the IP Act.<sup>70</sup> An agency discloses personal information if:

- it tells someone personal information or allows them to find it out; and
- that person didn't already know it or wasn't in a position to find it out on their own; and
- the agency won't have any control over what happens to the personal information.

Consideration should be given to the circumstances of each individual case when deciding if, and to whom, personal information might be released. Withholding a person's name may not be sufficient to protect that person's identity. Personal information can include any information or opinion from which a person's identity is apparent or may be 'reasonably ascertained'. For example, in a small agency or in a rural area, information about an employee's work area or location or even the type of complaint itself may be sufficient to identify that person. This should be taken into account when considering what information to release to a third party and whether to release it. The agencies selected for in-depth review addressed this issue explicitly.

**Example of guidance that can be provided regarding what information can be given when responding to a complaint**

DTMR has developed a fact sheet regarding what information may be given when responding to a complaint about an employee's behavior or conduct. The fact sheet discusses information privacy factors that need to be considered, such as the level of detail being considered for release, what happens if the employee's name is already known to the complainant and the seriousness of the complaint.

A copy of the fact sheet is available in Appendix 9.

<sup>68</sup> For example, the identity of the complainant is invariably a subject of interest to the person complained about. However, in many cases, this identity is not relevant to the subject matter of the complaint.

<sup>69</sup> For example, one outcome of a complaint is that the person complained about undergoes specialist training and that the complainant be assured that this training has occurred.

<sup>70</sup> Section 23 of the IP Act.

It should also be noted that the IP Act is subject to other Acts. This means that if another law requires the disclosure of personal information in a particular circumstance, that law takes precedence over the privacy obligations in the IP Act.

Examples of scenarios involving the disclosure about outcomes of a complaint are provided in Appendix 10.



The [OIC Guideline: Investigations, outcomes and complainants](#)<sup>71</sup> provides further guidance on how the type of complaint will affect whether giving information to a complainant will be a disclosure of personal information in breach of the privacy principles.

### 7.3 Access applications under the *Right to Information Act 2009* (Qld)

It is common for individuals who have made a complaint to an agency or individuals who have been the subject of a complaint to exercise their right to request access to government-held information and submit an access application under the *Right to Information Act 2009* (Qld) (**RTI Act**) or the IP Act for access to documents about, or arising out of, their complaint.

Schedule 4 of the RTI Act lists public interest factors for and against disclosure. Decision makers must identify all relevant public interest factors and balance them to decide if it would be contrary to the public interest to give access to documents.



The [OIC Guideline: Applications for investigation and complaint documents](#)<sup>72</sup> provides further guidance about the factors favouring disclosure and the factors favouring non-disclosure that commonly arise when processing applications for complaint documents.

<sup>71</sup> This document can be accessed from this link <http://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/investigations-outcomes-and-complainants>.

<sup>72</sup> This document can be accessed from this link <http://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/decision-making/applications-for-investigation-and-complaint-documents>.

In many cases, after applying the public interest balancing test, an agency might decide against providing access to complaint documents. Consequently, some applicants may choose to exercise their review rights and seek an internal or external review of the decision not to release documents.

To help agencies to manage the expectations of people applying for these documents, OIC has prepared a number of information sheets that outline issues that commonly arise on external review for people applying for documents about complaints.



The [OIC Information sheet: Applying for complaint documents](http://www.oic.qld.gov.au/guidelines/for-community-members/information-sheets-access-and-amendment/applying-for-complaint-documents)<sup>73</sup> explains the types of information that applicants are likely to receive. Including a copy of this information sheet when notifying an applicant of their review rights may help to manage expectations.

---

<sup>73</sup> This document can be accessed from this link  
<http://www.oic.qld.gov.au/guidelines/for-community-members/information-sheets-access-and-amendment/applying-for-complaint-documents>.

## 8 Management reporting on complaints

---

### **Privacy requirements**

#### **IPP10 - Limits on use of personal information (equates to NPP2)**

There are no IPP10 issues arising when an agency uses personal information for the purpose for which it obtained the information – termed the ‘primary use’. When information that was obtained for the purposes of dealing with a complaint is used for that complaint, this is a primary use.

Under IPP10, an agency must not use personal information for a purpose other than that for which it was obtained unless one of the exemptions in IPP10 is satisfied.

If the primary use is well-defined and articulated and the personal information is used exclusively in relation to that use, there will be no IPP10 issues. Lack of detailed information about primary purpose could lead to community concerns about a potential IPP10 breach. IPP10 also applies where an agency considers that the information is useful for another, unrelated agency function. Sometimes the secondary use will not have been contemplated when the data was initially obtained.

In many instances, if personal information is obtained in the course of dealing with a complaint, and then used again for a later complaint, this can be a ‘secondary purpose’ and would potentially be a breach of IPP10.

One of the exemptions in IPP10 allows secondary use of information where the purpose is ‘directly related’ to the earlier purpose. For earlier complaint material to be used for a new complaint, the two complaints must have a direct relationship. The fact that some of the parties are common to both complaints would not be sufficient to establish that relationship. IPP10(1)(e) provides conditions under which personal information may be used for a secondary purpose. Agencies seeking to ‘re-use’ complaint information for training and educative purposes will find it difficult to fit this use into the exemptions in IPP10. However, if the complaint material is suitably de-identified, there would be no use of personal information and accordingly, IPP10 would not apply.

## **Privacy requirements**

### **IPP5 - Providing information about documents containing personal information (equates to NPP5)**

IPP5 requires that an agency must take reasonable steps to ensure that a person can find out what personal information is held by the agency, the purpose for which the information is held and how an individual can obtain access to their personal information.

Complaints information is part of the information holdings of an agency. OIC's experience is that agency compliance with IPP5 in terms of complaint documentation is limited.<sup>74</sup> The general lack of information provided by agencies to the community about the agencies' personal information holdings could limit the extent to which individuals can exercise the rights of access afforded to them by the IP Act.

## **Key findings**

- Some agencies use a complaints management reporting template to ensure that information is no longer linkable to an identifiable individual when providing reports on the performance of the agency's CMS.
- Some agencies develop appropriately de-identified case notes from complaints data to assist staff in responding to common queries or to provide guidance on the application of the privacy principles in specific situations.
- Few agencies included information about the type of personal information contained in complaints documents and the main purposes for which this personal information is used in its list of personal information holdings.

## **8.1 Collecting personal information for a secondary purpose**

An effective CMS will have mechanisms in place to provide feedback to relevant areas of the agency where potential system improvements are identified.<sup>75</sup>

<sup>74</sup> The OIC *Results of Desktop audits 2011-12*, viewable at [http://www.oic.qld.gov.au/data/assets/pdf\\_file/0010/7795/results-of-desktop-audits-2011-12.pdf](http://www.oic.qld.gov.au/data/assets/pdf_file/0010/7795/results-of-desktop-audits-2011-12.pdf), found that 67 out of 147 (46%) of the agency websites reviewed had a privacy plan or policy, but not all plans were compliant with IPP5. OIC *Results of Desktop Audits 2012-13*, viewable at [http://www.oic.qld.gov.au/data/assets/pdf\\_file/0008/22310/report-results-of-desktop-audit-2012-13.pdf](http://www.oic.qld.gov.au/data/assets/pdf_file/0008/22310/report-results-of-desktop-audit-2012-13.pdf) continued to show limited progress with only 26 (31%) of the 83 agencies reviewed demonstrating compliance with IPP5 by publishing a list of personal information holdings.

<sup>75</sup> Queensland Ombudsman's *Effective Complaints Management Fact Sheet: Business Improvement*, viewable at

Personal information about parties to the complaint would not always be necessary as part of feedback about systems improvements.

A 'directly related purpose' is one which is closely associated with the original purpose, even if it is not strictly necessary to achieve that purpose. For example, where an agency uses information obtained for the purpose of providing a service, it would be reasonable to expect that the agency consequently uses this information for the further purpose of monitoring, evaluating, auditing or providing that service.

If personal information is required to be passed on from the CMS to other parts of an agency for the purposes of improving systems and practices, the personal information may be used for this secondary purpose if it is directly related to the primary purpose. It is often a component of the resolution of a complaint that shortfalls in systems or processes are rectified. While use of complaints data, individually or in aggregate form, to identify areas where the agency's business processes and systems could be improved is encouraged, it is good privacy practice that an agency uses only those parts of the personal information which are directly relevant to fulfilling this additional purpose.

For reporting purposes, if the complaint information is adequately de-identified, reports concerning those complaints do not attract the obligations of IPP10. Examples of good privacy practice in agencies' secondary use of personal information are provided below.

#### **Example of secondary use – Example A**

In DSITIA,<sup>76</sup> information from the electronic complaints register is reported by Executive, Legal and Integrity Services via quarterly reporting to the Assistant-Director General, Shared Services (for serious level 2 complaints<sup>77</sup>) and to the Board of Management (for very serious level 3 complaints<sup>78</sup>). The information provided in the executive reports is limited to the number and type of complaint, time taken to conclude complaints and highlights any significant trends and issues. A copy of DSITIA's quarterly complaints management reporting template is provided in Appendix 11.

---

<http://www.ombudsman.qld.gov.au/Publicagencies/Resources/EffectiveComplaintsManagement/ComplaintsManagementResources/EffectiveComplaintsManagementFactSheets/tabid/148/Default.aspx>

<sup>76</sup> DSITIA *Complaints management procedure*, viewed at <http://www.qld.gov.au/dsitia/assets/documents/complaints-management-procedure.pdf>, November 2013.

<sup>77</sup> Level 2 complaints are generally of a more complex or serious nature and could impact negatively on the department. Such complaints will require assessment and/or investigation. Examples of level 2 complaints include industry or customer dissatisfaction with an element of departmental operations; unsatisfactory program expenditure/progress; a departmental employee disclosed a client's personal information to a party outside the department.

### **Example of secondary use – Example B**

In DJAG, the complaint register includes an area to record corrective action and business improvement activities arising from a complaint. Corporate Governance prepares a complaints report to the Board of Management every six months, using complaints reports provided by managing officers and approved by the relevant divisional head. DJAG's *Client complaint management handbook*<sup>79</sup> suggests that analysis of complaints should include identifying:

- the number of complaints received:
  - simple, standard and complex complaints
- the issues:
  - service delivery, staff conduct, administrative decision, policy/procedure, privacy
- the number of finalised complaints
- the number of unresolved complaints
- any systemic issues or trends; and
- any business improvement opportunities either implemented during the period being reported on or for the future.

The in-depth review found that DTMR also provided comprehensive guidance on how to recognise a systemic issue. Addressing systemic issues often leads to business and service improvements, which will in turn prevent or reduce multiple or repeated complaints from recurring. A copy of DTMR's guidance on identifying systemic issues, significant issues and trends is provided in Appendix 12.

## **8.2 Use of case notes**

The in-depth review found that some agencies use complaint management data to develop suitably de-identified case notes or training examples to assist staff in responding to common queries or to provide guidance on the application of the privacy principles in specific situations. For example, RRC identified frequently asked requests for information handled by Council's Customer Service Centre, such as water meter readings, and

<sup>78</sup> Level 3 complaints are generally complex and significant in nature and could impact negatively on the department and/or cause lasting detriment. Such complaints will require comprehensive assessment and/or investigation. Examples of level 3 complaints include departmental action that has threatened the operations or viability of a private business or other government department; a business area disposed of copies of documents containing sensitive personal information in an unsecured manner resulting in a party outside the department gaining access to the files.

<sup>79</sup> Viewed December 2013.



updated its Customer Service Officer guidelines to include advice on the interpretation and application of the IP Act when responding to these types of requests.



OIC publishes a range of [case notes](#)<sup>80</sup> that illustrate application of IPPs and interpretation of the IP Act in a variety of subject areas.

When creating case notes, it is important that data is appropriately de-identified so that the information is no longer linkable to an identifiable individual. The simplest method of de-identification involves the removal of obvious identifiers such as an individual's name or address. However, stripping out obviously identifying information may not be sufficient and care needs to be taken to ensure that an individual's identity is not reasonably ascertainable by using or cross-referencing other available information with information used in the case note.



The [OIC Guideline: Dataset publication and de-identification techniques](#)<sup>81</sup> provides an introduction to the tools and techniques for de-identifying data so that its publication can comply with the privacy principles in the IP Act.

### 8.3 Personal information holdings

Agencies have an obligation under the IP Act<sup>82</sup> to take reasonable steps to ensure that the community is aware of the types of personal information held by an agency, what it is used for and how it can be accessed. Complaints management is a function for which an agency is likely to collect and use personal information.

One of the means by which an agency can meet this obligation is to include this information in the agency's privacy policy, or to publish an appropriately worded privacy plan, either on their website or in hard copy form upon request.

<sup>80</sup> These case notes can be accessed from this link <http://www.oic.qld.gov.au/information-for/information-privacy-officers/case-notes>

<sup>81</sup> This document can be accessed from this link <http://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/dataset-publication-and-de-identification-techniques>

<sup>82</sup> As required by IPP5 and NPP5.



The review identified that guidance is needed on providing information about an agency's **personal information holdings**. OIC will develop resources to provide further advice on how much detail to provide about the type of personal information held by an agency and the main purposes for which it is used.

## 9 Conclusion

---

Complaints generally can reflect distrust and conflict between the parties; these issues are compounded if the parties also distrust the complaints process. Perceived shortfalls in the complaint process and in particular in the information flows may lead to a fresh complaint. Managing privacy considerations properly can reduce the risk of privacy breaches and avoid the potential for privacy breaches to undermine community confidence in the complaint management process.

This review conducted an examination of privacy policy and practice in complaint management across 38 agencies in general terms and six agencies in-depth with the view to identifying instances where privacy compliance had been incorporated into complaints management systems.

The review found that generally agencies were mindful and respectful of privacy in their complaints process, although these practices were not necessarily formally documented and at times were inconsistently applied.

Aspects of good practice were noted in the agencies reviewed in-depth, and these have been outlined in this report as case studies or examples to assist other agencies in adopting similar practices.

It is intended that this report is used as the basis for a resource manual for good privacy practice in complaint handling.<sup>83</sup> The Office of the Information Commissioner will develop further guidance resources for agencies. The Office of the Information Commissioner will also use the report as a starting point for future compliance reviews of agency information privacy policy and practice in the area of complaint management.

The Office of the Information Commissioner recommends that agencies consider the good privacy practices identified in this report and incorporate these practices into their complaint management systems.

---

<sup>83</sup> Further complaint handling resources are provided in Appendix 13.



## **APPENDICES**



## Appendix 1 – Acronyms

---

CMS	Complaints Management System
DJAG	Department of Justice and Attorney-General
DSITIA	Department of Science, Information Technology, Innovation and the Arts
DTMR	Department of Transport and Main Roads
IP Act	<i>Information Privacy Act 2009 (Qld)</i>
IPP	Information Privacy Principle
IS18	Information Standard 18: Information Security
NPP	National Privacy Principle
OAIC	Office of the Australian Information Commissioner
OIC	Office of the Information Commissioner
QO	Queensland Ombudsman
RRC	Rockhampton Regional Council
RTI	Right to Information
RTI Act	<i>Right to Information Act 2009 (Qld)</i>





## **Appendix 2 – Terms of Reference**

---

### **Review of Complaint Handling Practices**

#### **1. Objectives of the Review**

- 1.1. The objective of the review is to examine and report on the extent to which complaint handling systems incorporate privacy considerations and adopt the privacy principles set out in the *Information Privacy Act 2009* (Qld) (**IP Act**), publicise examples of good practice, and identify areas of complaint practice requiring the development of privacy themed information resources

#### **2. Scope of the Review**

- 2.1. Data collected in the desktop audit will be used to form an initial view as to the extent to which publicly available complaint handling policies and publicly visible practices incorporate privacy considerations and adopt the privacy principles and identify agencies that appear likely to have a mature approach to the incorporation of privacy principles into complaint handling systems.
- 2.2. The in-depth review will examine agency complaint handling policies, documentation and training materials to assess each agency's capacity to consider privacy issues in the context of its complaint handling function, including:-
  - 2.2.1. Collection of information relevant to the complaint, notably but not limited to the information provided to participants in the complaint process about the collection and management of their personal information – Information Privacy Principles (IPP) 1-3.
  - 2.2.2. A review of policies governing the storage and security of complaint information – IPP4.
  - 2.2.3. Secondary use of personal information - for example if personal information is collected and used for one complaint, to what extent under the privacy principles can the information be used for a different complaint? – IPP10.
  - 2.2.4. Disclosure of personal information – not only to the immediate parties to the complaint and witnesses but also to any other entity involved with the complaint – IPP11.
  - 2.2.5. Bound contracted service providers – what privacy conditions are required to be in place where an agency outsources its complaint handling function, either wholly or on an individual complaint basis – Chapter 2, Part 4 of the IP Act.

#### **2.3. Suitability Criteria for Assessing Performance**

- 2.4. The review is based on an assessment of the performance of the agency against the requirements of the IP Act, and any subordinate guidelines or instruments made pursuant to the legislation.
- 2.5. Where the legislation states that the agency must meet a particular requirement, that requirement is considered to be an auditable element of the legislation. The review tests whether or not the agency has complied with that requirement.

- 2.6. Where the legislation indicates that the agency should adopt a particular approach, the review will make a qualitative assessment of the extent to which the agency has adopted that approach.

### **3. Assessment Process**

- 3.1. In conducting the review, the Acting Privacy Commissioner (Mr Lemm Ex) and the Manager, Performance Monitoring and Reporting (Ms Karen McLeod) will work with a review team including Senior Privacy Officers and Senior Performance, Monitoring & Reporting Officers. The review team will work through the testing program with your nominated staff to ensure that each relevant area of practice has been considered and appropriate evidence gathered to support findings. Appropriate evidence may be gathered through the following processes:

- 3.1.1. Examination of agency websites
- 3.1.2. Discussions with relevant staff and management
- 3.1.3. Examination of internal documentation including internal policies and procedures, training manuals and other instructional material and internal protocols
- 3.1.4. Examination of agency policies for and use of information arising from complaints
- 3.1.5. Examination of complaint management clauses in contracts with any service providers who manage complaints on behalf of the agency or as part of their dealings with the agency (as appropriate)
- 3.1.6. Examination of agency intranet; and
- 3.1.7. Review of statistical records/reporting.

### **4. Reporting**

- 4.1. The report will outline findings and make recommendations to improve agency personal information handling practices and systems, and will describe good examples of agencies' incorporation of privacy considerations into CMSs.

Issues identified during the review regarding the incorporation of privacy into agency CMSs for agencies reviewed in-depth will be raised progressively during the review with the relevant agencies.

Sections of the draft report concerning individual agency performance will be forwarded to the relevant agencies for comment.

Comments received will be considered for incorporation into the final report. This final report, together with any agency's formal response to recommendations, will be submitted to the Speaker of the Queensland Parliament, for tabling in the Legislative Assembly.

### **5. Administrative Matters**

#### **5.1. Timing**

At this stage, it is envisaged that the onsite review will be commence in mid-October and will be finalised by November 2013. The report drafting is anticipated to be concluded by December 2013, assuming circumstances do not intervene.

## Appendix 3 – Referral of a complaint to another agency fact sheet

Department of Transport and Main Roads

Human Resources and Governance Branch

Information Privacy

### Transfer of information between Queensland Government Agencies

This fact sheet is provided to assist employees of the Department of Transport and Main Roads (the department) when considering transferring correspondence or complaints between the department and other agencies. Employees of the department must comply with the 11 Information Privacy Principles (IPPs) contained in the *Information Privacy Act 2009* (IP Act) when collecting, using, storing or disclosing personal information.

In general, the department must only use personal information for the purpose for which it was collected and disclose personal information only where the individual concerned is aware of, or has consented to the disclosure or, where there is a legal requirement for that information to be disclosed.

#### What is personal information?

Personal information is any information that may lead to the identity of an individual. Personal information can be almost anything that is associated with a living individual. It can include correspondence, audio recordings, registration numbers and images.

For information to be personal information **two** criteria must be satisfied.

1. It must be about an individual.
2. The individual's identity must be reasonably ascertainable from the information or opinion.

#### Disclosure of personal information

The forwarding of information to a third party or another agency would involve passing personal information out of the control of the department. Any disclosure of personal information outside of the department must comply with IPP 11 – Disclosure of Personal Information. Under IPP 11, an agency must not disclose personal information to a third party, unless:

- the individual is reasonably likely to be aware of the disclosure
- the individual has expressly or impliedly agreed to the disclosure
- the disclosure is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual
- the disclosure is authorised or required under law
- the disclosure is necessary for law enforcement purposes
- the disclosure is necessary for research or statistical purposes.

#### Transferring correspondence between Queensland government agencies

##### Implied agreement


In some circumstances it may be appropriate for the department to rely on the consideration that the individual would reasonably likely to be aware that it is the agency's usual practice to disclose certain types of correspondence containing personal information.

For example, this approach may be appropriate in circumstances where the individual has identified a specific issue that they want rectified but they have misdirected their request to the wrong agency. In this situation it would be reasonable for the department to simply redirect the correspondence to the correct agency.

*Examples of where the department could reasonably refer correspondence for response by another organisation:*

- Where the department receives correspondence about an individual seen driving dangerously on a jet-ski, it would be appropriate to refer these complaints to the Queensland Police Service who have the authority to deal with these complaints.
- Where the department receives correspondence about a departmental service that is undertaken by a contractor, or work that is under the jurisdiction of another government agency, a council, government owned corporations (Queensland Rail), it would be appropriate and helpful to refer the correspondence to these agencies as the matter would require direct response from those organisations.

Great state. Great opportunity.



Office of Information Commissioner - Report to the Queensland Legislative Assembly No. 6 of 2013/14

Page 69

Implied agreement sets a high bar. It should not be used if there is any doubt as to whether the individual would agree if they were to be asked about the transfer of their complaint. It will be necessary for each division within the department to consider each matter on its own merits, and only after careful consideration of all relevant factors.

The department's employees must also take great care to ensure that the agency to where the correspondence is being re-directed is, in fact, the appropriate agency to deal with the subject matter of the correspondence. Care should also be taken in ensuring that the address which it is being re-directed to is correct.

*Example of when **NOT** to refer correspondence without consent or notification of the referral:*

- Correspondence is received from a person complaining about an individual, Member of Parliament or a private company for example. In this situation, the department would not transfer this to the person mentioned, but rather send a response back to the complainant advising that the matter can not be addressed by the department.

Bear in mind that any transfer of personal information outside of the department is considered a disclosure of information. The more sensitive the information, the greater the consequences will be if the information is inappropriately used or disclosed. If you are in any doubt as to whether the person would want their correspondence to be passed onto another agency, best practice is to contact them prior to the transfer of information and ascertain their requirements.

#### **When notification of a referral should be sent**

If it is appropriate that an individual's correspondence be passed onto another organisation for response or action, best practice would be to advise an individual that their correspondence has been transferred out of the department for actioning. This way, the individual is kept informed on where their personal information has been redirected to.

*Examples of wording that can be used to notify a person when referring their matter to another department/agency*

*"Thank you for your letter received on (date). Please be advised that the matter you have raised falls within the functions of (agency) and to assist you in this matter, we have forwarded your correspondence to that agency for it's response. Please contact (name of officer in other agency) on (phone number) for more information"*

*Referral of Ministerial correspondence to another Minister or agency*

*"I refer to (letter/email/facsimile) of (date) from (person, title and organisation) about (subject). As this matter falls under the jurisdiction of the Honourable (Minister's full name and title), I am referring the matter to you for consideration and direct reply. Enclosed are copies of the relevant correspondence for your attention."*

If you have any concerns about privacy in your area or have questions as to whether certain personal information should be used or disclosed, please ask your Manager or contact TMR's Privacy Contact Officer on (07) 3066 7566 or email [privacy@tmr.qld.gov.au](mailto:privacy@tmr.qld.gov.au).

#### **Your privacy contacts**


<b>Rachel Dando</b>	Principal Advisor Information Privacy	3066 7103
<b>Clara Foster</b>	Privacy Contact Officer	3066 7566
<b>Grasme Healey</b>	Director (RTI, Privacy and Complaints Management)	3066 7102
Email <a href="mailto:privacy@tmr.qld.gov.au">privacy@tmr.qld.gov.au</a>		

Legal and Ethical Standards, July 2013

**Connecting Queensland**  
delivering transport for prosperity

**13 QGov (13 74 68)**  
[www.tmr.qld.gov.au](http://www.tmr.qld.gov.au) | [www.qld.gov.au](http://www.qld.gov.au)

## Appendix 4 – Sample complaint form

Department of Justice and Attorney-General					
<b>Complaint form</b>					
<p><b>Your feedback is important to us.</b> If you are dissatisfied with our services or how they were provided to you, we want to make it easy for you to register a complaint with us. You can complete this form, or submit your complaint online at <a href="http://www.justice.qld.gov.au">www.justice.qld.gov.au</a></p>					
<b>Personal details</b>					
Preferred title:	Mr <input type="checkbox"/>	Mrs <input type="checkbox"/>	Miss <input type="checkbox"/>	Ms <input type="checkbox"/>	Other <input type="checkbox"/>
Last name:					
First name/s:					
<b>Contact details</b>					
What is your postal address?					
	Suburb				Postcode
Telephone:	Home ( )	Work ( )	Mobile		
Email address:					
Other ways to contact you:					
Preferred way for us to contact you:	Telephone <input type="checkbox"/>	Letter <input type="checkbox"/>	Email <input type="checkbox"/>	Other <input type="checkbox"/>	
<b>Complaint details</b>					
Are you a current employee of DJAG making this complaint?			Yes <input type="checkbox"/>	No <input type="checkbox"/>	
Have you raised your complaint with us before?			Yes <input type="checkbox"/>	No <input type="checkbox"/>	
<p>If yes, please tell us what business area you spoke to and when, who you spoke to, what you were told and why you are still dissatisfied. Please attach any documentation you have from your previous contact. Use a separate sheet if needed.</p>					
Does your complaint involve a breach of privacy?			Yes <input type="checkbox"/>	No <input type="checkbox"/>	
Have you done anything about your complaint already? (eg sought assistance from a solicitor or your local member of parliament)			Yes <input type="checkbox"/>	No <input type="checkbox"/>	
<p><b>Great state. Great opportunity.</b></p> 					

If yes, please advise details including the person you spoke to, when you spoke to them and the advice given.

#### Complaint summary

For **NEW** complaints, please tell us **what** business area you are making a complaint about; **when** and **where** it happened; **who** was involved; subject matter of the complaint (decision/action); copies of any documentation supporting your complaint; grounds of your complaint (why the action/decision is wrong); detriment suffered (how affected). If necessary, please attach an extra page to outline your complaint.

#### Please tell us what you would like to happen to resolve your complaint

#### Lodgement

You can lodge your completed form and any attachments by:

- posting it to:

Department of Justice and Attorney-General  
Include name of business area (if you know it)  
GPO Box 149  
Brisbane, QLD, 4000

Alternatively, go to [www.justice.qld.gov.au](http://www.justice.qld.gov.au) and submit your complaint online.

#### What happens next?

Once we receive your complaint, we will contact you within five working days of receiving your complaint to let you know what we will do and the expected time it will take to investigate your complaint.

We take your complaint seriously and will contact you regularly or when important matters arise to keep you up to date.

#### Your privacy

The Department of Justice and Attorney-General (DJAG) is collecting your personal information for the purposes of identifying and dealing with your complaint, in accordance with the Department's *Client Complaint Management Policy*. Your personal information may be forwarded to the business unit or region relevant to your complaint so your complaint can be addressed. Your personal information will not be provided to any person you are complaining about, unless it is specifically required to ensure your complaint is appropriately dealt with. Any use of your personal information will be limited to that necessary to investigate and respond to the issues raised in your complaint.

 [www.justice.qld.gov.au](http://www.justice.qld.gov.au)

The material presented in this publication is distributed by the Queensland Government for information only and is subject to change without notice. The Queensland Government disclaims all responsibility and liability (including liability in negligence) for all expenses, losses, damages and costs incurred as a result of the information being inaccurate or incomplete in any way and for any reason. © State of Queensland (Department of Justice and Attorney-General) 2012.



This section is for agency use only				
Date complaint received:	DD / MM / YYYY			
Receiving officer:				
Method of complaint:	In person <input type="checkbox"/>	Telephone <input type="checkbox"/>	Letter <input type="checkbox"/>	Email <input type="checkbox"/>
	Fax <input type="checkbox"/>	Web <input type="checkbox"/>	Correspondence (MCAR, DCAR) <input type="checkbox"/>	
Complaint resolved:	Yes <input type="checkbox"/>		No <input type="checkbox"/>	
	<i>Include details in Notes section</i>			
Referred to managing officer:				Date: DD / MM / YYYY
Interpreter assistance required?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Disability or special need?	Yes <input type="checkbox"/> No <input type="checkbox"/>
Notes – including summary of any advice provided to complainant on initial contact:				

**\*\*Use the *Complaint action record* to complete the complaint management process.\*\***





## Appendix 5 – Sample complaint intake form

Complaint intake form
<b>Complainant's personal details</b>
<p>When collecting person information ensure the complainant is provided with the following privacy notice:</p> <p><i>The department is collecting your personal information for the purpose of assessing and resolving your complaint. Your personal information will be disclosed within the department only as necessary for the management of your complaint. Your personal details will not be disclosed to any other third party or used for any other purpose without your consent, unless authorised or required by law.</i></p> <p>COMPLAINANT ADVISED OF PRIVACY NOTICE <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Title: _____ Last name: _____ First name: _____</p> <p>Address: _____ Post code: _____</p> <p>Telephone (home): _____ (work): _____ (mobile): _____</p> <p>Other ways to contact the complainant (e.g. facsimile, email): _____</p> <p>Preferred way to contact the complainant: _____</p> <p>Does the complainant have a special need (e.g. interpreter)?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No If yes, please specify: _____</p>
<b>Complaint details</b>
<p>Has the complainant raised the complaint with the department before? <input type="checkbox"/> Yes <input type="checkbox"/> No If yes, <b>Who</b> did the complainant speak with, <b>What</b> were they told and <b>Why</b> are they still dissatisfied? Request documentation from previous contact if available.</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>For <b>NEW</b> complaints, <b>What</b> happened, <b>Who</b> was involved, <b>When</b> and <b>Where</b> did it happen?</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>What would the complainant like to see happen as a result of their complaint?</p> <p>_____</p> <p>_____</p> <p>_____</p> <p>Method by which complaint was received: <input type="checkbox"/> Phone <input type="checkbox"/> Fax <input type="checkbox"/> Email <input type="checkbox"/> Letter <input type="checkbox"/> In person <input type="checkbox"/> Other _____</p> <p>Name of staff member who received complaint: _____</p> <p>Signature: _____ Date: ____/____/____</p> <p>Name of staff member who will be dealing with the complaint: _____</p>
<p><b>Reminder: Please retain this information securely. Information relating to complaints should be accessible only by those staff members whose duties require them to use the information.</b></p>



## Appendix 6 – Sample complaints register

										Complaint number*
										Date received
										Name of employee to whom complaint was made
										Service/employee area location
										Mode of complaint (email/letter/ telephone etc.)
										Level (1,2,3)
										Privacy notice given Y/N
										Nature of complaint
										Employee dealing with complaint
										Outcome/resolution
										Action taken
										Date complainant notified
										Method by which complainant notified
										Business improvements required Y/N
										Response time
										Complaints of a similar nature



## Appendix 7 – Sample complaints information sheet template

---

### **Descriptive title – the individual should understand when reading it that this is important to them**

*Why are you getting this information sheet?*

You have been given a copy of this information sheet because the agency is [doing X]. [X] involves you because [reason].

*What is the agency doing?*

The agency is doing [activity X]. As part of this activity it will ask you for your information. The agency may also generate information about you from the information you provide.

*What will the agency do with my information?*

The agency will do [A, B and C] with your information. [Some detail about how if appropriate/relevant.]

*Will the agency protect my information?*

Yes. Under the *Information Privacy Act 2009* the agency has obligations to protect your information from misuse, and from unauthorised access, use and disclosure.

Once your information is held by the agency it will be kept safe and only used or disclosed in accordance with the law.

*Is the agency going to give my information to anyone else?*

The agency will give some information about you to [type of entity or entity by name]. This information will be limited to [list the information which will be given to the entity. This should be the minimum needed to achieve the policy objective/required by law.]

*Is the agency allowed to give this information to someone else?*

Yes, if it is the agency's usual practice to give information about individuals to someone else and it tells you that it is going to do so. This is set out in the *Information Privacy Act 2009*.

In this case, it is the agency's usual practice to give the above information to [type of entity or named entity].

*Why is the agency giving my information to someone else?*

[In simple terms set out the policy or legislative reasons why the information is going to be disclosed.]

*Who can I talk to if I have questions about any of this?*

[Put in contact details of who the individual can talk to.]

*Where can I find out more information about the agency's policies and practices?*

[Contact details or a website address which contains this information, for example relevant section of the agency's publication scheme.]



## Appendix 8 – Sample contract provisions

---

The examples provided below should not be relied on as legal advice. OIC suggests that agencies may wish to seek legal advice to determine what requirements to incorporate into formal contract arrangements to bind contracted service providers.

### Example A – City of Gold Coast

#### 21 Privacy and Personal Information

21.1 If the Contractor collects or has access to Personal Information in order to provide the Goods and/or Services, the Contractor must:

- (a) if the Principal is an 'agency' other than the health department within the meaning of the *Information Privacy Act 2009 (Qld)*, comply with Parts 1 and 3 of Chapter 2 of that Act in relation to the discharge of its obligations under the Contract, as if the Contractor was the Principal;
- (b) if the Principal is the 'health department' within the meaning of the *Information Privacy Act 2009 (Qld)*, comply with Parts 2 and 3 of Chapter 2 of that Act in relation to the discharge of its obligations under the Contract, as if the Contractor was the Principal;
- (c) ensure that the Personal Information is protected against loss and against unauthorised access, use, modification, disclosure or other misuse;
- (d) not use Personal Information other than for the purposes of the supply of the Goods and/or performance of the Services, unless required or authorised by law;
- (e) not disclose Personal Information without the consent of the Principal, unless required or authorised by law;
- (f) not transfer Personal Information outside of Australia without the consent of the Principal;
- (g) ensure that access to Personal Information is restricted to those of its employees and officers who require access in order to perform their duties under the Contract;
- (h) ensure that its officers and employees do not access, use or disclose Personal Information other than in the performance of their duties under the Contract;
- (i) ensure that its agents and sub-contractors who have access to Personal Information comply with obligations the same as those imposed on the Contractor under this Clause 21;
- (j) fully co-operate with the Principal to enable the Principal to respond to applications for access to, or amendment of a document containing an individual's Personal Information and to privacy complaints; and
- (k) comply with such other privacy and security measures as the Principal reasonably advises the Contractor in writing from time to time.

21.2 The Contractor must, if specified in item 20 of Schedule A, or if requested by the Principal during the Contract Term, obtain from its officers, employees, agent and/or sub-contractors engaged for the purposes of the Contract, an executed deed of privacy in a form acceptable to the Principal.

21.3 The Contractor must immediately notify the Principal on becoming aware of any breach of Clause 21.1.

## Example B – RRC



### **25.1 Compliance with privacy laws**

The Supplier must process all Personal Information in connection with this Agreement in accordance with the Privacy Laws (regardless of whether or not the Supplier is otherwise obliged to comply with the Privacy Laws) and only for the purposes of performing its obligations under this Agreement.

### **25.2 Compliance with directions of council**

The Supplier must comply with all reasonable requests or directions of Council in connection with the obligations of Council under the Privacy Laws or in connection with policies developed by Council from time to time for the purpose of complying with the Privacy Laws.

### **25.3 Permitted disclosures**

- (a) The Supplier must not disclose Personal Information collected for the purposes of this Agreement without the prior authority of Council unless the disclosure is required:
  - (i) for the purposes of performing its obligations under this Agreement; or
  - (ii) by Legislative Requirements.
- (b) The Supplier must immediately notify Council where it becomes aware that a disclosure of Personal Information may be required by law.

### **25.4 Transfer of information outside of Australia**

The Supplier must not transfer outside Australia Personal Information collected for the purposes of this Agreement, or allow parties outside Australia to have access to such Personal Information, without the prior approval of Council.

### **25.5 Protection of personal information**

The Supplier must take all necessary steps to ensure that Personal Information collected for the purposes of this Agreement is protected against loss and against unauthorised access, use, modification, disclosure or other misuse and that only personnel authorised by Council have access to the Personal Information.

### **25.6 Supplier to notify of breaches**

The Supplier must notify Council immediately if it becomes aware of a breach of any of clauses 25.1 to 25.5 by the Supplier or any Personnel or employee of any Personnel.



## Appendix 9 – Information Privacy considerations when responding to complaints about employees fact sheet

Department of Transport and Main Roads

Human Resources and Governance Branch

Information Privacy

### Considering Information Privacy when responding to complaints about employees

All complaints regarding personal information or suspected breaches of privacy must be referred to the RTI, Privacy and Complaints Management Team, Legal and Ethical Standards.

This fact sheet will provide guidance to managers regarding what information may be given when responding to complaints about an employee's behaviour or conduct.

#### The Queensland Information Privacy Act 2009

The Information Privacy Act 2009 (Old) (IP Act) regulates the handling of personal information held by Queensland government agencies. The IP Act contains 11 information privacy principles (IPPs) which are designed to protect the right to privacy by:

- regulating the way we collect, store, use and disclose information about people;
- allowing people access to their information; and
- allowing people to request changes to that information when it becomes out of date or inaccurate.

#### What is personal information?

Personal information is any information that may lead to the identity of an individual. Personal information can be almost anything that is associated with a living individual. It can include correspondence, audio recordings, registration numbers and images.

For information to be personal information two criteria must be satisfied.

1. It must be about an individual.
2. The individual's identity must be reasonably ascertainable from the information or opinion.

#### What is routine personal work information?

The personal information of an employee, such as their name, signature and position title is found in almost all documents held by agencies. This is referred to as routine personal work information.

While this information can be considered to be personal information, it is generally released to members of the public under Right to Information or IP Act applications, as the infringement of an employees' right to privacy would generally be minimal or non-existent.

#### What is NOT routine personal work information?

Any information that is not related wholly to the routine day to day work activities of an employee cannot be considered as routine personal work information, regardless of whether it may arise out of a work context, for example:

- complaints made by or about an employee
- reasons why an employee is accessing leave entitlements of any kind or when they have taken, or intend to take, leave
- the fact that an employee has been unsuccessful in applying for a position
- details about an employee's family or private life.


#### What information privacy factors should you consider when responding to complaints?

Personal information relating to the investigation of a complaint must be handled within the boundaries set by the IP Act. In most circumstances, it should be possible to give a complainant adequate information about the way their complaint has been handled without disclosing personal information about an employee.

#### What level of detail is being considered for release?

Personal information can include any information or opinion from which a person's identity is apparent or may be 'reasonably ascertained'. For example, in a small town or rural area, information about an employee's work area or location, or even the type of complaint itself, may be sufficient to identify that person. This should be taken into account when considering what level of detail to release to a complainant.

Great state. Great opportunity.



**What if the employee has been specifically named by the complainant?**

Where an employee has been specifically named, the complainant will invariably be aware of the employee's identity. However, this does not mean that any additional personal information about the employee (such as any disciplinary action imposed) can, or should be, disclosed to the complainant.

**Is there a concern about the welfare of the employee?**

Consideration should be given to any adverse effects that disclosure of an employee's personal information might have on the employee. For example; rumours of their misconduct becoming widespread or a complainant using that information in a way that impacts negatively on the employee. Or does the employee have existing personal circumstances that should be taken into consideration?

**What is the seriousness of the complaint?**

Some kinds of misconduct, such as ongoing lack of respect and courtesy in dealing with the public, may call for wider dissemination of the results of an investigation and any sanctions imposed, remedial action taken or changes to policies or processes. These cases should always be referred to the local HR Advisor.

**Educating staff**

In some instances, there may be a need to highlight particular cases (such as unnecessary browsing of the department's customer records) for the purposes of raising awareness within the department. General information about the behaviour and the consequences of a case would be sufficient for this purpose, without the need to disclose specific personal information about an employee or a complainant. Care should be taken, particularly in smaller work teams, that an employee's identity cannot be 'reasonably ascertained' from any information provided in training or education material.

**Information Privacy Complaints and Breaches**

The department has complaint handling responsibilities under the IP Act. Individuals may complain if they believe their personal information has not been properly managed. Failure to protect the personal information collected from employees or members of the public may become the subject of a hearing and orders in the Queensland Civil and Administrative Tribunal.

**Managers should not be responding to privacy complaints.** All information privacy complaints, including allegations about a TMR employee's mishandling of an individual's personal information, should be referred directly and immediately to the Privacy Contact Officer on 3066 7568. This allows the department to conduct a proper investigation and a response to the complainant, including their review rights in the event they are dissatisfied with the department's findings.

Where a complaint about privacy is received, please fax it urgently to 3066 7101, with any originals being forwarded to:

The Privacy Contact Officer  
Legal and Ethical Standards  
Department of Transport and Main Roads  
Level 5, Capital Hill Building  
85 George Street  
Brisbane Qld 4001

or

The Privacy Contact Officer  
Legal and Ethical Standards  
Department of Transport and Main Roads  
GPO Box 1549  
Brisbane Qld 4001

For more information about information privacy, please contact the Privacy Contact Officer on 3066 7568 or via e-mail at [privacy@tmr.qld.gov.au](mailto:privacy@tmr.qld.gov.au)

**Your privacy contacts**

Rachel Dando	Principal Advisor Information Privacy	3066 7103
Clare Foster	Privacy Contact Officer	3066 7568
Graeme Healey	Director (RTI, Privacy and Complaints Management)	3066 7102
Email	<a href="mailto:privacy@tmr.qld.gov.au">privacy@tmr.qld.gov.au</a>	

Legal and Ethical Standards, July 2013

Connecting Queensland  
delivering transport for prosperity

13 QGov (13 74 68)  
[www.tmr.qld.gov.au](http://www.tmr.qld.gov.au) | [www.qld.gov.au](http://www.qld.gov.au)

## **Appendix 10 – Scenarios: Providing information on outcomes**

---

### **Scenario 1: Releasing information to a complainant where the employee is known**

An agency receives a complaint about the conduct of one of its employees. The complainant is aware of the employee's name, having met him and received a letter signed by him. The person making the complaint alleges that they have suffered financial detriment and loss of social standing because of the employee's actions.

The agency conducts an investigation and concludes that the allegation has been sustained and that a breach of the agency's procedures has occurred. The officer handling the complaint would like to inform the complainant that the employee has breached the agency's procedures and that disciplinary action has been taken. The complaints officer would also like to disclose the details of the disciplinary action.

#### ***Q: Can the agency release this information to the complainant?***

A: If, prior to an investigation, the agency envisages that the information it is about to collect in response to an incident will involve the collection of personal information from an employee, the first critical step is to notify the employee *in writing* that their personal information may be collected for the purpose of conducting the investigation and that the information might be disclosed to the person making the complaint. Prior to disclosing this information to the complainant, the employee could also be given the opportunity to make a case as to why their personal information should not be disclosed.

While such notice is a requirement under IPP2, it is also important that if it is envisaged that any personal information about the employee might be used or disclosed, such uses or disclosures will only be permitted if they comply with the agency's obligations under IPP11.

Therefore, if the agency has notified the individual that their personal information may be collected for the purpose of conducting the investigation or inquiry, and that it was possible that the information might be disclosed, it is likely that the disclosure will be permitted under IPP11(1)(a).

The complaints officer should consider whether the complainant can be advised about the outcome of the investigation without specifically mentioning the disciplinary action that has been imposed. It may be sufficient in this case for the complaints officer to advise that a

breach had been determined and action taken to rectify the situation. In other words, the level of detail may not need to be as great as the complaints officer is suggesting.

### **Scenario 2: Complainant seeking information on an investigation from an agency**

A member of the public lodges a complaint to an agency about the actions of an employee with whom he dealt when seeking assistance. The complainant claims that the employee asked intrusive questions in a harassing way, placing the complainant under pressure. The agency investigated and found that the employee's actions were within the agency's guidelines relating to obtaining client information. The agency advises the complainant that the matter had been investigated and the outcome finalised.

Later, the complainant finds out that the employee is still working at the agency and that she may have even been promoted. The complainant considers this unacceptable and complains to the agency. The agency confirms that the employee is still a staff member. The complainant then asks the agency what action it took following the original complaint and the agency advises that it cannot disclose this information for privacy reasons.

#### ***Q: Is the agency correct in refusing to provide information to the complainant?***

A: If the agency has determined, in the course of its investigation, that some of the information to be disclosed is personal information about the employee and that, in their view, this should not be disclosed under IPP11(1)(a), it should make its reasoning clear to the complainant.

Agencies should also note that there is no obligation placed on them under IPP11(1)(a) *notice to the individual* or (1)(b) *consent of the individual*, to provide personal information about an employee to a complainant. It is at the discretion of the agency.

In the interests of transparency, the agency should explain to the complainant how the IP Act works, why it came to its decision and why it considers it was appropriate to use this provision of the IP Act to not disclose personal information about the employee to the complainant.

*Importantly*, nothing in IP Act prevents the agency providing general information to a complainant as to how it dealt with their complaint. The agency should reiterate that it has undertaken an investigation of the complaint and that, in its view, the employee concerned is not at fault. The agency may choose to provide general information regarding processes or training, or to advise that no finding of fault has been attributed.

If the complainant can be assured that the agency fully considered the lawfulness of disclosing the information and demonstrated that a thorough investigation had been undertaken, the complainant is less likely to consider the agency's response to be a 'cover-up'. This can be done without releasing any personal information.

### **Acknowledgement**

In developing these scenarios, OIC acknowledges the advice produced by the Australian Public Service Commission: [Circular 2008/3: Providing information on Code of Conduct investigation outcomes to complainants](http://www.apsc.gov.au/publications-and-media/circulars-and-advice/2008/circular-20083).<sup>84</sup>

---

<sup>84</sup> Viewable at <http://www.apsc.gov.au/publications-and-media/circulars-and-advice/2008/circular-20083>



## Appendix 11 – Sample performance reporting template

### Suggested quarterly reporting template

#### Quarterly complaints management reporting

##### Purpose

To provide the Assistant Director-General, Shared Services with the details of level 2 complaints for [Division] for the quarter ended [date].

##### Background

The [Division] is committed to effectively handling complaints in a timely and professional manner.

This report advises the number and nature of level 2 complaints including service/product related complaints, privacy complaints, as well as complaints regarding [Division] employees.

This report also advises the time taken to conclude complaints and highlights any significant trends and issues.

#### Level 2 complaints

##### Summary

Number of complaints outstanding from previous quarter	Number of new complaints lodged this quarter	Number of complaints finalised this quarter	Total number of complaints outstanding at end of quarter

##### Nature of new level 2 complaints this quarter

Type/subject of complaint	Number of new complaints this quarter	Percentage of new complaints
Service/product (cost)		%
Service/product (quality)		%
Service/product (time)		%
Service/product (other)		%
Staff (conduct)		%
Staff (skill/knowledge)		%
Staff (other)		%
Other (e.g. privacy)		%
		%

##### Time taken to conclude the level 2 complaints finalised this quarter

Timeframes	Number	Percentage	Comments
Within 30 business days		%	
Longer than 30 business days		%	
		%	

##### Trends and issues

Significant trends or issues for attention .....

A large proportion of complaints this quarter related to concerns regarding .....

Additional analysis indicates that .....

Recommendations have been made to ..... and therefore .....

The following business improvement recommendations are outstanding at the end of the current quarter:





## Appendix 12 – Identifying systemic issues, significant issues and trends fact sheet

---

Department of Transport and Main Roads

### Guide for: identifying systemic issues, significant issues and trends

This guide is intended for branch complaints coordinators and any staff who collate or analyse complaints. It provides guidance on how to identify possible systemic issues, significant issues and trends. This analysis can help identify valuable information such as high risk issues, seasonal trends, commonalities and improvements. It can also explain some of the reasons why we get multiple, repeated or even escalated complaints.

For questions on this guide, contact the RTI, Privacy and Complaints Management Team, Legal and Ethical Standards Unit (Human Resources and Governance Branch) by emailing the 'complaints policy' inbox or calling Vanessa Coker (07 3066 0732) or Kate Holzapfel (07 3066 7589).

More information about the reporting process can be found in the *Complaints Management Procedures* and the *Frequently asked questions – Quarterly complaints reporting*.

Click on the links to the common questions below to find out more information:

- [What is a systemic issue?](#)
- [What is not a systemic issue?](#)
- [How to recognise a systemic issue](#)
- [What is a significant issue?](#)
- [How to recognise a significant issue](#)
- [What is a trend?](#)
- [How to review a trend](#)
- [Tips for preparing your general complaints data](#)
- [Finding more information](#)
- [What to do next](#)

#### **What is a systemic issue?**

[BACK TO TOP](#)

A systemic issue is the failure of a product, service, system, policy or procedure which causes or leads to a complaint. It commonly occurs when the product, service, system, policy or procedure:

- doesn't exist in TMR; or
- does exist but it's faulty, incorrect, inadequate or inappropriate.

The effects in both cases are:

- customer needs or expectations are not met
- the intended purpose, objective or outcome is not achieved
- there is no clear guidance, consistency or efficiency.

#### **For example**

*The TMR website doesn't have an online payment service for handwritten infringement notices. The only option for a customer is to make payment via money order or cheque. This lack of accessible services doesn't meet customer needs or the expectation that TMR should keep current with changed technology.*

#### **For example**

*TMR has a complaints management policy however the internal review provisions are inadequate. The processes outlined are too general resulting in inconsistencies with how the process is applied. The policy doesn't provide sufficient guidance to staff and doesn't meet its intended purpose.*

#### **What is not a systemic issue?**

[BACK TO TOP](#)

A systemic issue isn't a human error, an error in a staff member's judgement or a one off oversight or incident which involves specific or isolated factors.

Great state. Great opportunity.



*For example*

*A typing mistake when entering a customer's details into a database is a simple human error. If however, the error continues to occur, particularly with multiple staff members, there may be an underlying design flaw with the useability of the database or inadequate processes in place to check and ensure the quality of data entered.*

*For example*

*A staff member's error in judgement when assessing eligibility under the school transport assistance scheme policy is likely an isolated error which is often corrected easily at the local level through training. If however, recurring substantial or widespread mistakes are made, this may highlight an underlying issue with the adequacy of training protocols or reveal a lack of appropriate processes in place to manage application approvals.*

### **How to recognise a systemic issue**

[BACK TO TOP](#)

A systemic issue is normally caused by an underlying or fundamental problem and may be identified:

- during the course of investigating an individual complaint; or
- when collated complaints are reviewed (may be a single complaint or a pattern of repeated complaints).

When reviewing complaints data, look at the root cause of the complaint/s to understand:

- why the complaint/s occurred
- what factors contributed to the complaint/s
- how the issue/s or problem/s can be corrected
- how the complaint could have been prevented.

Consider if the root cause involves a product, service, system, policy or procedure and examine whether any one of these is inadequate, inappropriate, faulty or non-existent. Look at whether changing or improving the product, service, system, policy or procedure may have prevented the complaint in the first place.

Once a failure is identified, action should be taken to rectify the problem or improve the situation. Often complaints are investigated in isolation and action is taken to only fix the effects or result of the systemic problem, not the actual cause or fundamental issue. This results in complaints being received again and again.

*For example*

*Numerous complaints received about registration labels not sticking. For each customer, the complaint is managed and a new label issued however there is an underlying problem with the new glue used by the manufacturer. If this problem was not identified and properly addressed, complaints would continue to be received.*

### **What is a significant issue?**

[BACK TO TOP](#)

A significant issue is any information that is important for TMR. It is significant enough that it may:

- need to be escalated or brought to the attention of management e.g. a high risk issue or hot topic.
- help raise awareness or understanding with staff or management e.g. a key learning or outcome.
- provide valuable background or context to a complaint/s.

### **How to recognise a significant issue**

[BACK TO TOP](#)

There are two types of significant issues:

- 1) Issues involving a single complaint that may need to be escalated or that raises awareness. These are often classified as 'intermediate' or 'complex' due to the nature of the issue/s or its implication/s.

*For example*

- a high risk issue e.g. allegations about TMR's administration or interpretation of safety legislation/ policy and whether TMR contributed to the injury of a vessel crew member.
- a hot topic or an in focus issue e.g. the commencement of a new project that may impact on culturally significant land requiring negotiations/ discussions with the traditional land owners.
- a key learning or outcome e.g. a review into the use of non traditional reversing beepers on project related machinery to minimise impact to local residents.
- an escalated complaint e.g. a complaint which has been through internal review and is now pending external review with the Queensland Ombudsman's Office.

- 2) Issues which arise from multiple complaints, particularly if there is some important background or history with possible risk or wider implications.

*For example*

- a number of seemingly insignificant complaints that are part of a wider number of requests about the same issue.
- a high number of complaints which are actually pro-forma template letters e.g. from a lobby group.
- complaints that are triggered by an unexpected or unplanned action, decision or event.
- repeat complaints that may escalate e.g. due to petitions, action groups, media attention.

Investigating significant issues will often reveal business and service improvements. Keep in mind however a significant issue may not be a complaint which raises a 'red flag'. Not all complaints are important or urgent. Sometimes a significant issue starts from a seemingly minor complaint which involves some other factor, such as a repeated pattern of complaints, some contentious history of the complaint or its potential to escalate.

### **What is a trend?**

[BACK TO TOP](#)

A trend is any pattern, commonality or key observation found in complaints. This is usually found in an increase or decrease with complaints of the same nature:

- in a single quarter
- over multiple quarters
- across seasonal periods.

### **How to review a trend**

[BACK TO TOP](#)

Analysing trends can highlight wider or underlying issues and can provide a better understanding of how your business operates. This can then be used to reduce or prevent future complaints. The following three steps outline how to review a potential trend.

Firstly, determine what type of trend it is, such as a sudden spike, gradual increase or seasonal fluctuation.

*For example*

- sudden spike attributed to TMR e.g. technical issues on the website resulting in an outage of the online service for registration payments.
- sudden spike not attributed to TMR e.g. an incorrect media report on a possible policy change on the number of required learner driver log book hours.
- gradual increase over multiple quarters e.g. related to the phased roll out of a new but unpopular mandatory product.
- seasonal fluctuation within annual quarters attributed to TMR e.g. the yearly increase in public transport fares.
- seasonal fluctuation within annual quarters not attributed to TMR e.g. related to the cyclone and wet season.

Then think about what may have caused or contributed to the trend, such as a decision, action or inaction.

*For example*

- the decision to change a TMR policy that adversely affects customer licensing requirements.
- an action to close roads during peak hour causing congestion on a major route.
- an inaction to address boat ramp repairs which resulted in a safety incident.

Finally establish whether there is an underlying problem within the complaint.

*For example*

- the failure of a TMR product e.g. poor quality of public transport fare cards.
- inadequate service e.g. a design flaw where the online form is unable to accept overseas addresses.
- an out of date policy e.g. there are no provisions in place to reflect changed technology.

### **Tips for preparing your general complaints data**

[BACK TO TOP](#)

Collating particular complaints together can help with analysis, especially if there is a large volume of complaints data. By grouping complaints by location, interest or topic, you may get a better understanding of the main issues or reveal commonalities that aren't initially obvious.



*For example, searching by:*

- location details e.g. project name, regional area, specific office or service centre, unit or team.
- particular focus areas e.g. increased fees from a policy change or a new customer form and service introduced.
- key topic e.g. practical driver licensing tests or call centre wait times.

Sorting your complaints by common type or into a logical order can give a quick snapshot into how the data is broken up and it may help prioritise which complaints to follow up and investigate further.

*For example, sort by:*

- classification e.g. focus on any potential high risk intermediate or complex complaints.
- complaint type e.g. to get a better understanding of where the main complaints come from.
- timeliness e.g. to see how the area or branch is tracking and identify any overdue complaints.
- anonymous complaints e.g. to check if there's a reason why the customer wishes to remain anonymous.
- internal review e.g. focus on any complaints that may escalate and check if these were managed appropriately.

### **Finding more information**

[BACK TO TOP](#)

Seek assistance from a subject matter expert, a policy area, technical area, manager or local complaints coordinator. They may have first hand knowledge or be able to provide additional information. The RTI, Privacy and Complaints Management Team can also assist with analysing complaints, trends or issues.

Having an overall awareness of TMR news and events that happen may assist you to understand some of the complaints your business receives. The Communication Hub (on insideTMR) collates daily media clips about TMR as a resource. Noting down any issues relating to your branch throughout the quarter may be beneficial.

### **What to do next**

[BACK TO TOP](#)

Information gained from systemic or significant issues and trends should be used to determine an appropriate action to prevent or reduce complaints from occurring, recurring or escalating. Actions can be corrective and/ or preventative and may involve immediate remedial tasks to fix an isolated issue or involve broader remedies.

*For example*

- action to repair a large pothole caused by unexpected flooding which poses a high risk safety issue.
- an alternative solution to reduce the impact of noise on residents by rearranging the schedule of planned works.
- a departmental review to examine the quality a manufactured TMR product.

Action should be monitored until completion and assessed for effectiveness to identify any relevant learnings.

*For example*

- monitoring corrective road works for the pothole to ensure safety standards are met and to determine preventative measures for future wet seasons.
- following up with residents near the project to ensure the change in works schedule has addressed the noise issue and to determine if the solution may be applicable to other projects.
- implementing the outcomes of the product review to ensure specifications are met and to determine improvements to quality control measures.

As systemic issues, significant issues and trends often lead to business and service improvements that benefit customers as well as TMR, they should be reported appropriately. This may include bringing an issue to the attention of a manager, general manager or reporting it within your branch's quarterly complaints.

## **Appendix 13 – Further complaint handling resources**

---

The following information security resources may be relevant to entities:

### **Queensland Ombudsman**

In addition to assessing and investigating complaints, the Queensland Ombudsman (**QO**) has an administrative improvement role, providing training and advice to help agencies improve decision-making and administrative practice.

QO publishes a range of complaints management resources, including a fact sheet series and self-audit checklist. QO also provides complaints management training that is designed to help Frontline Officers and Internal Review Officers manage complaints more effectively.

QO also has an ongoing program of targeted compliance reviews, focusing on the operation of CMS.

For more information, contact the Queensland Ombudsman on:

Telephone: (07) 3305 7000 or freecall 1800 068 908

Website: [www.ombudsman.qld.gov.au](http://www.ombudsman.qld.gov.au)

Email: [ombudsman@ombudsman.qld.gov.au](mailto:ombudsman@ombudsman.qld.gov.au)

### **Crime and Misconduct Commission**

The Crime and Misconduct Commission 'Facing the facts', a guide for dealing with suspected official misconduct in Queensland public sector agencies. The guidelines detail how to:

- plan an investigation
- maintain the integrity of the process; and
- ensure confidentiality and fairness.

The guide is available for download from the Crime and Misconduct Commission website:

[www.cmc.qld.gov.au](http://www.cmc.qld.gov.au)