Queensland

Information Privacy Act 2009

Current as at [Not applicable]

Indicative reprint note
This is an ***unofficial*** version of a reprint of this Act that incorporates all proposed amendments to the Act included in the Information Privacy and Other Legislation Amendment Bill 2023. This indicative reprint has been prepared for information only—***it is not an authorised reprint of the Act***.

Amendments to this Act are also included in the Integrity and Other Legislation Amendment Bill 2023 and the Public Records Bill 2023. These proposed amendments are not included in this indicative reprint.

The point-in-time date for this indicative reprint is the introduction date for the Information Privacy and Other Legislation Amendment Bill 2023—12 October 2023.

Detailed information about indicative reprints is available on the **Information** page of this website.

Queensland

Information Privacy Act 2009

Contents

		Page
Chapter 1	**Preliminary**	
Part 1	**Introductory**	
1	Short title	9
2	Commencement	9
3	Object of Act	9
6	Scope of personal information under this Act	9
7	Relationship with other laws regulating personal information	10
8	Relationship with other Acts regulating disposal of information	10
10	Act binds State	10
Part 2	**Interpretation**	
11	Definitions	11
12	Meaning of personal information	11
13	Meaning of held or holds in relation to personal information	11
15	Meaning of document	11
16	Meaning of document to which the privacy principles requirements do not apply	11
18	Meaning of agency	12
20	Special provision about application of Act to a Minister	12
21	Meaning of public authority	13
23	What it means to disclose personal information and to use personal information	14
24	References to doing an act or engaging in a practice	15
Chapter 2	**Queensland privacy principles**	
Part 1	**Compliance with QPPs by agencies**	
26	Queensland privacy principles	15
27	Agencies to comply with QPPs	16
28	Noncompliance with particular QPPs	16

Contents

29	Special provision for law enforcement agencies	16
Part 2	**Disclosure of personal information outside Australia**	
33	Disclosure of personal information outside Australia	17
Part 3	**Compliance with parts 1 and 2 and s 41 by contracted service providers**	
34	Meaning of service arrangement	18
35	Binding a contracted service provider to privacy principle requirements	19
36	Bound contracted service provider to comply with privacy principle requirements	20
37	Contracting agency to comply with privacy principles if contracted service provider not bound	21
Part 5	**Provision of information to Ministers**	
38	Personal information relevant to portfolio responsibilities	21
Part 6	**Miscellaneous**	
39	Nature of rights created by pts 1 to 3	21
Chapter 3	**QPP codes and guideline for permitted general situations**	
Part 1	**QPP codes**	
40	QPP codes	22
41	Agencies must comply with QPP codes	22
42	Preparing QPP codes	22
43	Approval of QPP codes or amendments of QPP codes	23
Part 2	**Guideline for permitted general situations**	
44	Preparing guideline	24
45	Approval of guideline	24
Chapter 3A	**Mandatory notification of data breaches**	
Part 1	**Preliminary**	
46	Application of chapter	25
47	Meaning of eligible data breach	25
Part 2	**Assessment of suspected eligible data breaches**	
48	Obligations of agencies in relation to data breaches	27
49	Extension of period for assessment by agency	28
Part 3	**Notifying eligible data breaches**	
Division 1	**Preliminary**	
50	Application of part	29
Division 2	**Notification**	
51	Agency must give statement about eligible data breach to information	

	commissioner	29
52	Further information to be provided	30
53	Agencies must notify particular individuals	31
54	Particular agencies may collect, use and disclose relevant personal information for notification	32
Division 3	**Exemptions**	
55	Exemption—investigations and proceedings	34
56	Exemption—eligible data breach of more than 1 agency	35
57	Exemption—agency has taken remedial action	35
58	Exemption—inconsistency with confidentiality provision	36
59	Exemption—serious risk of harm to health or safety	36
60	Exemption—compromise to cybersecurity	37
Part 4	**Role of information commissioner**	
61	Information commissioner may direct agency to give statement and make recommendations	38
Part 5	**Investigations**	
Division 1	**Authorised officers**	
62	Functions	39
63	Appointment	39
64	Identity cards	39
65	Production or display of identity card	40
66	Return of identity card	40
Division 2	**Entry of places occupied by agencies**	
67	General power to enter places occupied by agency	40
68	Information commissioner must give written notice of entry	41
Division 3	**Powers of authorised officers after entering places**	
69	General powers	42
70	Power to require reasonable help	42
71	Offence to contravene help requirement	43
Part 6	**Miscellaneous**	
72	Agency must keep register	43
73	Agency must publish data breach policy	44
74	Evidential immunity for individuals complying with particular requirements	44
Chapter 4	**Information Commissioner and Privacy Commissioner**	
Part 1	**Functions of information commissioner under this Act**	
134	Information commissioner not subject to direction	45

Contents

135	Performance monitoring, investigation and support functions	46
136	Decision-making functions	47
138	Power to issue guidelines	48
Part 2	**Staff of Office of Information Commissioner in relation to this Act**	
139	Delegation	48
140	Staff subject only to direction of information commissioner	49
Part 3	**Privacy Commissioner**	
141	The Privacy Commissioner	49
142	Role and function of privacy commissioner	49
143	Privacy commissioner subject to direction of information commissioner 49	
144	Appointment	50
145	Procedure before appointment	50
146	Term of appointment	50
147	Remuneration and conditions	50
148	Leave of absence	51
149	Preservation of rights if public service officer appointed	51
150	Restriction on outside employment	51
151	Resignation	52
152	Acting privacy commissioner	52
Part 4	**Proceedings**	
153	Third party proceedings	53
154	Costs in proceedings	53
155	Information commissioner and privacy commissioner may appear in proceedings	54
156	Intervention by Attorney-General	54
Part 5	**Waiving or modifying particular obligations in the public interest**	
157	Applying for waiver or modification of particular obligations	54
Part 6	**Compliance notices**	
158	Compliance notice	55
159	Extension of time for compliance	56
160	Relevant entity must comply with notice	57
161	Application to Queensland Civil and Administrative Tribunal for review of decision to give compliance notice	57
162	Parties to QCAT proceeding	57
163	How QCAT may dispose of review	57
Chapter 5	**Privacy complaints**	

Part 1 **Making privacy complaints**

164 Meaning of privacy complaint 58

164A Response period for privacy complaints 59

165 Privacy complaint may be made or referred to information commissioner 59

166 Requirements for privacy complaint to information commissioner 60

166A Requirements for privacy complaint to relevant entity 61

Part 2 **Dealing with privacy complaints**

167 Preliminary action 62

168 Information commissioner may decline to deal with or to deal further with complaint 62

169 Referral of privacy complaint to other entity 63

170 Arrangement with ombudsman 64

Part 3 **Mediation of privacy complaints**

171 Attempting resolution through mediation 65

172 Certification of mediated agreement 65

173 Filing of certified agreement with Queensland Civil and Administrative Tribunal 66

173A Confidentiality of mediation 66

Part 4 **Referral of privacy complaints to QCAT**

174 Application of pt 4 66

175 Advice to parties 67

175A Complainant's request for referral to Queensland Civil and Administrative Tribunal 67

176 Referral to Queensland Civil and Administrative Tribunal 67

177 Parties to QCAT proceeding 68

178 How QCAT may dispose of complaint 68

Chapter 6 **Protections and offences**

Part 1 **Protections**

179 Access—protection against actions for defamation or breach of confidence 69

181 Access—protection in respect of offences 70

183 Protection of agency, information commissioner etc. from personal liability 70

Part 2 **Offences**

184 Direction to act in particular way 71

185 Unlawful access 71

186 False or misleading information 71

Contents

187	Failure to give information or attend proceedings	72
188	Disclosure or taking advantage of information	72
Chapter 7	**Miscellaneous provisions**	
Part 2	**Operation of this Act**	
192	Review of Act	73
193	Reports of information commissioner	74
194	Report to Assembly on Act's operation	75
195	Functions of parliamentary committee	75
Part 3	**Other**	
196	Power of person acting for another person	76
196A	Information commissioner may make preliminary inquiries	77
197	Power of information commissioner to require information or attendance	77
199	Exchange of information	78
199A	Corporations legislation displacement	79
200	Approval of forms	80
201	Regulation-making power	80
Chapter 8	**Transitional provisions**	
Part 1	**Transitional provisions for Act No. 14 of 2009**	
202	Delayed application of Act other than ch 3 to local governments	80
203	Outdated references	80
204	Pre-enactment recruitment process	81
205	Refusal to deal with application—previous application for same documents	81
206	Delayed filing of certified agreement with QCAT	81
207	Delayed referral of privacy complaint to QCAT	81
208	Delayed application to QCAT	81
209	Privacy complaints to relate to actions after ch 5 commencement	82
210	Continuing application of relevant information standards	82
211	Acts and practices authorised before relevant date	83
Part 2	**Transitional provisions for State Penalties Enforcement and Other Legislation Amendment Act 2009**	
212	Definition for pt 2	83
213	Retrospective validation for particular delegations and directions	83
214	Decision under s 69(2) is a reviewable decision	84
Part 3	**Transitional provisions for Information Privacy and Other Legislation Amendment Act 2023**	

215	Definitions for part	84
216	Existing bound contracted service providers	85
217	Existing access and amendment applications	85
218	Continued protection for giving access to or publishing chapter 3 documents	86
219	Delayed application of ch 3A to local governments	87
220	Existing approvals under former s 157	87
221	Existing compliance notices under s 158	87
222	Information commissioner may issue compliance notice for failure to comply with former IP Act	87
223	Privacy complaints about act or practice of relevant entity not yet made before commencement	88
224	Privacy complaints made but not finalised before commencement	88
225	Continuation of sections 185 and 187 for chapter 3 documents	89
226	Report to Assembly on Act's operation	89
Schedule 1	**Documents to which the privacy principle requirements do not apply**	90
1	Covert activity	90
2	Witness protection	90
3	Disciplinary actions and misconduct	90
4	Public interest disclosure	91
5	Cabinet and Executive Council	91
6	Commissions of inquiry	91
7	Other	91
Schedule 2	**Entities to which the privacy principle requirements do not apply** 92	
Part 1	**Entities to which the privacy principle requirements do not apply**	
Part 2	**Entities to which the privacy principle requirements do not apply in relation to a particular function**	
Schedule 3	**Queensland privacy principles**	94
Part 1	**Consideration of personal information privacy**	
1	QPP 1—open and transparent management of personal information	94
2	QPP 2—anonymity and pseudonymity	96
Part 2	**Collection of personal information**	
3	QPP 3—collection of solicited personal information	96
4	QPP 4—dealing with unsolicited personal information	98
5	QPP 5—notification of the collection of personal information	99
Part 3	**Dealing with personal information**	

6	QPP 6—use or disclosure of personal information	100
7	QPP 7—direct marketing	103
8	QPP 8—cross-border disclosure of personal information	103
9	QPP 9—adoption, use or disclosure of government related identifiers 103	
Part 4	**Integrity of personal information**	
10	QPP 10—quality of personal information	104
11	QPP 11—security of personal information	104
Part 5	**Access to, and correction of, personal information**	
12	QPP 12—access to personal information	105
13	QPP 13—correction of personal information	105
Schedule 4	**Permitted general situations and permitted health situations**	108
Part 1	**Permitted general situations**	
1	Collection, use or disclosure	108
Part 2	**Permitted health situations**	
2	Collection—provision of a health service	109
3	Collection—research etc.	110
4	Use or disclosure—research etc.	111
5	Disclosure—responsible person for an individual	111
Schedule 5	**Dictionary**	113

Information Privacy Act 2009

An Act to provide safeguards for the handling of personal information in the public sector environment

Chapter 1 Preliminary

Part 1 Introductory

1 Short title

This Act may be cited as the *Information Privacy Act 2009*.

2 Commencement

This Act commences on a day to be fixed by proclamation.

3 Object of Act

(1) The primary object of this Act is to provide for the fair collection and handling in the public sector environment of personal information.

(2) The Act must be applied and interpreted to further the primary object.

6 Scope of personal information under this Act

This Act applies to the collection of personal information, regardless of when it came into existence, and to the storage, handling, accessing, amendment, management, transfer, use

and disclosure of personal information regardless of when it was collected.

7 Relationship with other laws regulating personal information

(1) This Act is intended to operate subject to the provisions of other Acts regulating—

(a) the collection, storage, handling, accessing, amendment, management, transfer and use of personal information; or

(b) the disclosure, within the meaning of section 23, of personal information.

(2) Without limiting subsection (1), the operation of QPPs 6.1 and 6.2(d) and the permitted health situation mentioned in schedule 4, section 5 do not override any law with respect to assisted and substituted decision-making, including, for example, the *Guardianship and Administration Act 2000* and *Powers of Attorney Act 1998*.

8 Relationship with other Acts regulating disposal of information

This Act does not affect the provisions of other Acts regulating the disposal of information (however described).

Note—

See, for example, the *Public Records Act 2002*, section 13.

10 Act binds State

This Act binds the State.

Part 2 Interpretation

11 Definitions

The dictionary in schedule 5 defines particular words used in this Act.

12 Meaning of *personal information*

Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion—

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

13 Meaning of *held* or *holds* in relation to personal information

Personal information is ***held*** by a relevant entity, or the entity ***holds*** personal information, if the personal information is contained in a document in the possession, or under the control, of the relevant entity.

15 Meaning of *document*

In this Act, a ***document*** does not include a document to which the privacy principle requirements do not apply.

16 Meaning of *document to which the privacy principles requirements do not apply*

In this Act, a ***document to which the privacy principle requirements do not apply*** means a document mentioned in schedule 1.

18 Meaning of *agency*

(1) In this Act, an ***agency*** means—

(a) a Minister; or

(b) a department; or

(c) a local government; or

(d) a public authority.

(2) However, in this Act, ***agency*** does not include an entity to which the privacy principle requirements do not apply.

(3) For this Act—

(a) a board, council, committee, subcommittee or other body established by government to help, or to perform functions connected with, an agency is not a separate agency, but is taken to be comprised within the agency; and

(b) a reference to an agency includes a reference to a body that is taken to be comprised within the agency; and

(c) a reference to local government includes a reference to the Wide Bay Water Corporation.

(4) In this section—

entity to which the privacy principle requirements do not apply means—

(a) an entity mentioned in schedule 2, part 1; or

(b) an entity mentioned in schedule 2, part 2 in relation to the function mentioned in that part.

20 Special provision about application of Act to a Minister

If a provision of this Act applies to a Minister, the provision applies only for acts done, or practices engaged in, as the case may be, in the Minister's capacity as a Minister in relation to the affairs of an agency administered by the Minister.

21 Meaning of *public authority*

(1) In this Act, ***public authority*** means any of the following entities—

Note—

Under the *Acts Interpretation Act 1954*, schedule 1—

entity includes a person and an unincorporated body.

(a) an entity—

(i) established for a public purpose by an Act; or

(ii) established by government under an Act for a public purpose, whether or not the public purpose is stated in the Act;

(b) an entity created by the Governor in Council or a Minister;

(c) another entity declared by regulation to be a public authority for this Act, being an entity—

(i) supported directly or indirectly by government funds or other government assistance; or

(ii) over which government is in a position to exercise control; or

(iii) established under an Act; or

(iv) given public functions under an Act;

(d) subject to subsection (5), a person holding an office established under an Act;

(e) a person holding an appointment—

(i) made by the Governor in Council or Minister otherwise than under an Act; and

(ii) declared by regulation to be an appointment the holder of which is a public authority for this Act.

(2) Despite subsection (1), ***public authority*** does not include an entity established by letters patent.

(3) For subsection (1)(c), an entity may be declared by regulation to be a public authority for this Act in relation to only a part of the entity's functions.

(4) A prescribed entity is not a public authority in relation to documents received, or created, by it in performing a function other than the public function given under an Act.

(5) A person is not a public authority merely because the person holds—

(a) an office the duties of which are performed as duties of employment as an agency's officer; or

(b) an office of member of a body; or

(c) an office established under an Act for the purposes of an agency.

(6) In this section—

prescribed entity means an entity that is a public authority only because it is given public functions under an Act and is declared by regulation to be a public authority for this Act.

23 What it means to *disclose* personal information and to *use* personal information

(1) An entity (the ***first entity***) ***discloses*** personal information to another entity (the ***second entity***) if—

(a) the second entity does not know the personal information, and is not in a position to be able to find it out; and

(b) the first entity gives the second entity the personal information, or places it in a position to be able to find it out; and

(c) the first entity ceases to have control over the second entity in relation to who will know the personal information in the future.

(2) An entity ***uses*** personal information if it—

(a) manipulates, searches or otherwise deals with the information; or

(b) takes the information into account in the making of a decision; or

(c) transfers the information from a part of the entity having particular functions to a part of the entity having different functions.

(3) Subsection (2) does not limit what actions may be ***use*** of the personal information.

(4) However, ***use*** of the personal information does not include the action of disclosing the personal information to another entity.

24 References to doing an act or engaging in a practice

In this Act, a reference to doing an act or engaging in a practice in contravention of a requirement includes a reference to a failure to act or a failure to engage in a practice in contravention of the requirement.

Chapter 2 Queensland privacy principles

Part 1 Compliance with QPPs by agencies

26 Queensland privacy principles

(1) Each Queensland privacy principle (***QPP***) is set out in schedule 3.

(2) In this Act, a reference to a QPP followed by a number is a reference to the provision of schedule 3 having that number.

27 Agencies to comply with QPPs

(1) An agency, other than an APP entity, must comply with the QPPs.

Note—

For the application of the Act in relation to a Minister, see also section 20.

(2) Without limiting subsection (1), the agency must not do an act or engage in a practice that contravenes, or is otherwise inconsistent with, a requirement of a QPP.

(3) An act or practice mentioned in subsection (2) includes any act or practice relating to the agency's collection, storage, handling, accessing, amendment, management, transfer, use or disclosure of personal information.

(4) In this section—

APP entity means an agency that is required to comply with the APPs.

28 Noncompliance with particular QPPs

(1) An agency is not required to comply with a prescribed QPP in relation to an individual's personal information if the information is related to or connected with personal information of the individual that has previously been published, or given for the purpose of publication, by the individual.

(2) In this section—

prescribed QPP means QPP 6 or 10.2.

publish, for personal information, means publish the information by way of television, newspaper, radio, internet or other form of communication.

29 Special provision for law enforcement agencies

(1) A law enforcement agency is not subject to QPP 3.6, 5, 6 or 10.1, but only if the law enforcement agency is satisfied on

reasonable grounds that noncompliance with the QPP is necessary for—

(a) if the enforcement agency is the Queensland Police Service—the performance of its activities related to the enforcement of laws; or

(b) if the enforcement agency is the Crime and Corruption Commission—the performance of its activities related to the enforcement of laws and its intelligence functions; or

(c) if the enforcement agency is the community safety department—the containment, supervision and rehabilitation of offenders under the *Corrective Services Act 2006* and the supervision of prisoners subject to supervision orders or interim supervision orders under the *Dangerous Prisoners (Sexual Offenders) Act 2003*; or

(d) if the enforcement agency is any other law enforcement agency—the performance of its responsibility mentioned in schedule 5, definition *law enforcement agency*, paragraph (b)(iv), including the conduct of proceedings started or about to be started in a court or tribunal in relation to the responsibility.

(2) In this section—

intelligence functions means the functions mentioned in the *Crime and Corruption Act 2001*, section 53.

Part 2 Disclosure of personal information outside Australia

33 Disclosure of personal information outside Australia

An agency may disclose an individual's personal information to an entity outside Australia only if—

(a) the individual agrees to the disclosure; or

(b) the disclosure is authorised or required under a law; or

(c) the agency is satisfied on reasonable grounds that the disclosure is 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

(d) 2 or more of the following apply—

(i) the agency reasonably believes that the recipient of the personal information is subject to a law, binding scheme or contract that effectively upholds principles for the fair handling of personal information that are substantially similar to the QPPs;

(ii) the disclosure is necessary for the performance of the agency's functions in relation to the individual;

(iii) the disclosure is for the benefit of the individual but it is not practicable to seek the agreement of the individual, and if it were practicable to seek the agreement of the individual, the individual would be likely to give the agreement;

(iv) the agency has taken reasonable steps to ensure that the personal information it discloses will not be held, used or disclosed by the recipient of the information in a way that is inconsistent with the QPPs.

Part 3 Compliance with parts 1 and 2 and s 41 by contracted service providers

34 Meaning of *service arrangement*

(1) In this Act, a ***service arrangement*** is a contract or other arrangement entered into after the commencement of this section under which an entity other than an agency (the

contracted service provider) agrees or otherwise arranges with an agency (the ***contracting agency***) to provide services.

(2) For subsection (1)—

(a) the services must be for the purposes of the performance of 1 or more of the contracting agency's functions; and

(b) the services must be provided either—

(i) directly to the contracting agency; or

(ii) to another entity on the contracting agency's behalf; and

(c) the contracted service provider must not be in the capacity of employee of the contracting agency in providing the services.

35 Binding a contracted service provider to privacy principle requirements

(1) An agency entering into a service arrangement must take all reasonable steps to ensure that the contracted service provider is required to comply with parts 1 and 2 and section 41, as if it were the agency, in relation to the discharge of its obligations under the arrangement.

(2) However, the agency must comply with subsection (1) only if—

(a) the contracted service provider will in any way deal with personal information for the contracting agency; or

(b) the provision of services under the arrangement will involve—

(i) the transfer of personal information to the contracting agency; or

(ii) the provision of services to a third party for the contracting agency.

(3) The agency is not required to comply with subsection (1) if—

(a) the contracted service provider is to receive funding from the contracting agency; and

(b) the contracted service provider will not collect personal information for the contracting agency; and

(c) the contracted service provider will not receive any personal information from the contracting agency for the purposes of discharging its obligations; and

(d) the contracted service provider will not be required to give the contracting agency any personal information it collects in discharging its obligations.

(4) Subsections (1) to (3) are not intended to limit what may be provided for in a service arrangement about the contracted service provider's collection, storage, handling, accessing, amendment, management, transfer, use or disclosure of personal information, whether or not the contracted service provider is a bound contracted service provider.

36 Bound contracted service provider to comply with privacy principle requirements

(1) A bound contracted service provider under a service arrangement must comply with parts 1 and 2 and section 41 in relation to the discharge of its obligations under the arrangement as if it were the entity that is the contracting agency.

(2) The requirement to comply under subsection (1) continues to apply to the bound contracted service provider in relation to personal information it continues to hold after its obligations under the service arrangement otherwise end.

(3) A bound contracted service provider's compliance with the privacy principle requirements may be enforced under this Act as if it were an agency.

(4) Subsections (1) to (3) are not intended to prevent a service arrangement from including a requirement for the contracted service provider to comply with all or part of the privacy principles even though this part does not require that the service arrangement include the requirement.

37 Contracting agency to comply with privacy principles if contracted service provider not bound

(1) This section applies if a contracted service provider under a service arrangement is not a bound contracted service provider because the contracting agency under the service arrangement did not take the steps required of it under section 35.

(2) The obligations that would attach to the contracted service provider if it were a bound contracted service provider attach instead to the contracting agency under the arrangement.

Part 5 Provision of information to Ministers

38 Personal information relevant to portfolio responsibilities

An agency does not contravene the requirement under this Act that it comply with the QPPs only because it gives personal information to a Minister to inform the Minister about matters relevant to the Minister's responsibilities in relation to the agency.

Part 6 Miscellaneous

39 Nature of rights created by pts 1 to 3

(1) Except as provided for under the procedures set out in this Act, an obligation imposed on an entity under part 1, 2 or 3 does not—

(a) give rise to any civil cause of action; or

(b) operate to create in any person any legal right enforceable in a court or tribunal.

(2) Subsection (1) does not limit chapter 5.

Chapter 3 QPP codes and guideline for permitted general situations

Part 1 QPP codes

40 QPP codes

(1) A ***QPP code*** is a written code of practice about information privacy, approved by regulation under section 43, that states—

(a) how 1 or more of the QPPs are to be applied or complied with; and

(b) the agencies that are bound by the code, or a way of determining the agencies that are bound by the code.

(2) A QPP code may also impose additional requirements to those imposed by a QPP, to the extent the additional requirements are not inconsistent with a QPP.

(3) A QPP code expires on the earlier of the following days—

(a) the day that is 5 years after the day the QPP code is approved under section 43;

(b) if the QPP code states an expiry day—the stated day.

41 Agencies must comply with QPP codes

An agency must not do an act, or engage in a practice, that contravenes a QPP code that is in effect and binds the agency.

42 Preparing QPP codes

(1) The information commissioner or an agency may prepare a draft QPP code or draft amendment of a QPP code and submit the draft to the Minister for endorsement.

(2) However, before the information commissioner or agency submits the draft code or amendment to the Minister, the commissioner or agency must—

(a) publish the draft on an accessible agency website; and

(b) invite the public to make submissions to the commissioner or agency about the draft within a stated period of at least 20 business days; and

(c) consider any submissions made within the stated period.

(3) An agency must, immediately after publishing a draft QPP code or draft amendment of a QPP code under subsection (2), notify the information commissioner of the publication.

43 Approval of QPP codes or amendments of QPP codes

(1) This section applies if a draft QPP code or draft amendment of a QPP code is submitted to the Minister under section 42.

(2) If the draft is submitted by an agency, the Minister must ask the information commissioner for submissions about the draft.

(3) The Minister must decide to endorse or refuse to endorse the draft, having regard to—

(a) any submissions made by the information commissioner; and

(b) any other relevant matter.

(4) If the Minister endorses the draft, the Minister must recommend to the Governor in Council the making of a regulation approving the QPP code or amended QPP code.

(5) The QPP code or amended QPP code—

(a) does not take effect unless it is approved by regulation; and

(b) takes effect on the day prescribed by regulation for the code or amended code.

(6) The information commissioner must, as soon as practicable after a regulation approving a QPP code or amended QPP

code is made, publish the code or amended code on the commissioner's website.

Part 2 Guideline for permitted general situations

44 Preparing guideline

(1) The information commissioner may—

(a) prepare a draft guideline about the collection, use or disclosure of personal information to assist an entity locate a person who has been reported as missing; and

(b) submit the draft to the Minister for endorsement.

(2) However, before the information commissioner submits the draft guideline to the Minister, the commissioner must—

(a) publish the draft on the commissioner's website; and

(b) invite the public to make submissions to the commissioner about the draft within a stated period of at least 20 business days; and

(c) consider any submissions made within the stated period.

45 Approval of guideline

(1) This section applies if a draft guideline is submitted to the Minister under section 44.

(2) The Minister must decide to endorse or refuse to endorse the draft.

(3) If the Minister endorses the draft, the Minister must recommend to the Governor in Council the making of a regulation approving the guideline.

(4) The guideline—

(a) does not take effect unless it is approved by regulation; and

(b) takes effect on the day prescribed by regulation for the guideline; and

(c) expires 5 years after the day mentioned in paragraph (b).

(5) The information commissioner must, as soon as practicable after a regulation approving a guideline is made under this section, publish the guideline on the commissioner's website.

Chapter 3A Mandatory notification of data breaches

Part 1 Preliminary

46 Application of chapter

(1) This chapter applies in relation to personal information, other than personal information in a document to which the privacy principle requirements do not apply, held by an agency.

(2) However, this chapter does not apply to an agency that is an APP entity under the *Privacy Act 1988* (Cwlth).

47 Meaning of *eligible data breach*

(1) An ***eligible data breach*** of an agency is a data breach of the agency that occurs in relation to personal information held by the agency if—

(a) both of the following apply—

(i) the data breach involves unauthorised access to, or unauthorised disclosure of, the personal information;

(ii) the access or disclosure is likely to result in serious harm to an individual (an ***affected individual***) to

whom the personal information relates, having regard to the matters stated in subsection (2); or

(b) the data breach involves the personal information being lost in circumstances where—

(i) unauthorised access to, or unauthorised disclosure of, the personal information is likely to occur; and

(ii) if the unauthorised access to or unauthorised disclosure of the personal information were to occur, it would be likely to result in serious harm to an individual (also an ***affected individual***) to whom the personal information relates, having regard to the matters stated in subsection (2).

(2) For subsection (1)(a)(ii) and (b)(ii), the matters are—

(a) the kind of personal information accessed, disclosed or lost; and

(b) the sensitivity of the personal information; and

(c) whether the personal information is protected by 1 or more security measures; and

(d) if the personal information is protected by 1 or more security measures—the likelihood that any of those security measures could be overcome; and

(e) the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information; and

(f) the nature of the harm likely to result from the data breach; and

(g) any other relevant matter.

Part 2 Assessment of suspected eligible data breaches

48 Obligations of agencies in relation to data breaches

(1) This section applies in relation to a data breach of an agency if the agency knows, or reasonably suspects, that the data breach is an eligible data breach of the agency.

(2) The agency must—

(a) immediately take all reasonable steps to contain the data breach; and

(b) if the agency does not know whether the data breach is an eligible data breach of the agency—assess whether there are reasonable grounds to believe the data breach is an eligible data breach of the agency.

(3) An assessment under subsection (2)(b) must be completed within—

(a) 30 days after the suspicion mentioned in subsection (1) was formed; or

(b) if the period mentioned in paragraph (a) is extended under section 49—the extended period.

(4) After becoming aware or forming the reasonable suspicion of the eligible data breach, including during an assessment of the data breach under subsection (2)(b), the agency must—

(a) take, or continue to take all reasonable steps to contain the data breach, and take all reasonable steps to mitigate the harm caused by the data breach; and

(b) if the agency is aware the data breach may affect another agency—give a written notice to the other agency of the data breach that includes—

(i) a description of the data breach; and

(ii) a description of the kind of personal information the subject of the data breach, without including any personal information in the description.

(5) The agency need not comply with subsections (2)(b) and (3) in relation to the data breach if—

(a) all of the personal information the subject of the data breach is also the subject of a data breach of 1 or more other agencies; and

(b) at least 1 of the other agencies has undertaken to conduct the assessment in relation to the data breach.

49 Extension of period for assessment by agency

(1) This section applies if an agency required to conduct an assessment under section 48 is satisfied the assessment can not reasonably be completed within the 30 day period mentioned in section 48(3)(a).

(2) The agency may extend the period within which the assessment must be completed.

(3) If the period is extended under subsection (2), the agency must, within the 30 day period mentioned in section 48(3)(a)—

(a) start the assessment; and

(b) give a written notice to the information commissioner stating—

(i) that the assessment has started; and

(ii) the period within which the assessment must be completed has been extended under this section; and

(iii) the day the extended period ends.

(4) The information commissioner may ask the agency to provide further information or updates about the progress of the assessment.

Part 3 Notifying eligible data breaches

Division 1 Preliminary

50 Application of part

(1) This part applies if an agency reasonably believes that there has been an eligible data breach of the agency.

(2) However, division 2 does not apply in relation to the agency to the extent an exemption applies to the agency under division 3.

Division 2 Notification

51 Agency must give statement about eligible data breach to information commissioner

(1) The agency must, as soon as practicable after forming the belief mentioned in section 50—

(a) prepare a statement that includes the information stated in subsection (2); and

(b) give the statement to the information commissioner.

(2) For subsection (1)(a), the statement must, to the extent it is reasonably practicable, include the following information—

(a) the information that must be included in a notification given under section 53(2)(a) to (e), (h) and (i);

(b) a description of the kind of personal information the subject of the data breach, without including any personal information in the description;

(c) the agency's recommendations about the steps individuals should take in response to the data breach;

(d) whether the agency is reporting on behalf of other agencies affected by the same data breach and, if so, the details of the other agencies;

(e) the total number or, if it is not reasonably practicable to work out the total number, an estimate of the total number of each of the following—

(i) all individuals affected or likely to be affected by the data breach;

(ii) affected individuals for the data breach;

(f) either—

(i) the total number of individuals notified of the data breach or, if it is not reasonably practicable to work out the total number, an estimate of the total number; or

(ii) if section 57 is relied on, the total number of individuals who would have been notified if that section had not been relied on or, if it is not reasonably practicable to work out the total number, an estimate of the total number;

(g) whether the individuals notified have been advised about how to make a privacy complaint to the agency under section 166A.

52 Further information to be provided

(1) This section applies if it is not reasonably practicable to include any information required under section 51 when the statement is given to the information commissioner under that section, including, for example, the total number of individuals mentioned in section 51(2)(e) or (f).

(2) The agency must take all reasonable steps to provide the information to the commissioner as soon as practicable after the statement is given.

53 Agencies must notify particular individuals

(1) The agency must, as soon as practicable after the belief mentioned in section 50 is formed—

(a) if it is reasonably practicable to notify each individual whose personal information has been accessed, disclosed or lost—take reasonable steps to notify each individual of the information mentioned in subsection (2); or

(b) if paragraph (a) does not apply and it is reasonably practicable to notify each affected individual for the data breach—take reasonable steps to notify each affected individual of the information mentioned in subsection (2); or

(c) if paragraphs (a) and (b) do not apply—publish the information mentioned in subsection (2) on an accessible agency website for a period of at least 12 months, other than information that would prejudice the agency's functions.

(2) A notification under subsection (1) must, to the extent it is reasonably practicable, include the following information—

(a) the name of the agency and, if more than 1 agency was affected by the data breach, the name of each other agency;

(b) the contact details of the agency or a person nominated by the agency for the individual to contact in relation to the data breach;

(c) the date the data breach occurred;

(d) a description of the data breach, including the type of eligible data breach under section 47;

(e) information about how the data breach occurred;

(f) for a notification under subsection (1)(a) or (b)—

(i) a description of the personal information the subject of the data breach; and

(ii) the agency's recommendations about the steps the individual should take in response to the data breach;

(g) for a notification under subsection (1)(c)—

(i) a description of the kind of personal information the subject of the data breach, without including any personal information in the description; and

(ii) the agency's recommendations about the steps individuals should take in response to the data breach;

(h) if the data breach involved unauthorised access to or disclosure of personal information—the period during which the access or disclosure was available or made;

(i) the steps the agency has taken or will take to contain the data breach and mitigate the harm caused to individuals by the data breach;

(j) information about how an individual may make a privacy complaint to the agency under section 166A.

(3) The agency must, as soon as practicable after a notice is published under subsection (1)(c), provide the information commissioner with information about how to access the notice.

(4) The information commissioner must, after receiving the information under subsection (3), publish on the commissioner's website information about how to access the notice for a period of at least 12 months.

54 Particular agencies may collect, use and disclose relevant personal information for notification

(1) A regulation may prescribe—

(a) an agency (a ***disclosing agency***) that may, under this section, disclose relevant personal information to another agency; and

(b) an agency (a ***receiving agency***) that may, under this section, collect and use relevant personal information from a disclosing agency and disclose relevant personal information to the disclosing agency.

(2) A disclosing agency may disclose relevant personal information held by the agency to a receiving agency if the receiving agency is the subject of an eligible data breach.

(3) The receiving agency may collect and use relevant personal information from a disclosing agency, and disclose relevant personal information to the disclosing agency, if it is reasonably necessary for the purpose of confirming—

(a) the name and contact details of a notifiable individual; or

(b) whether a notifiable individual is deceased.

(4) A disclosing agency or receiving agency is not required to comply with a QPP in relation to the disclosure, collection or use of relevant personal information under this section.

(5) For subsection (2), an eligible data breach includes—

(a) a data breach that an agency reasonably believes is an eligible data breach; and

(b) a suspected data breach of an agency mentioned in section 61(1), whether or not the information commissioner has made a recommendation under section 61(4).

(6) If a disclosing agency may, under an Act, enter into an arrangement and charge a fee for the provision of personal information kept by the agency under that Act, the agency may do so under that Act in relation to personal information that may be disclosed under this section.

(7) In this section—

identifier, for an individual, means an identifier other than solely the individual's name, including, for example, a number, that is—

(a) assigned to the individual in relation to the individual's personal information by an entity for the purpose of uniquely identifying that individual, whether or not it is subsequently used other than in relation to the personal information; or

(b) adopted, used or disclosed in relation to the individual's personal information by an entity for the purpose of uniquely identifying the individual.

notifiable individual means—

(a) an individual mentioned in section 53(1)(a) or (b); or

(b) an individual the information commissioner recommends should be notified under section 61(4).

relevant personal information means the following information about an individual—

(a) the name of the individual;

(b) the contact details of the individual;

(c) the date of birth of the individual;

(d) an identifier for the individual;

(e) if the individual is deceased—the date of the individual's death.

Division 3 Exemptions

55 Exemption—investigations and proceedings

An agency need not comply with division 2 to the extent complying with that division is likely to prejudice—

(a) an investigation that could lead to the prosecution of an offence; or

(b) proceedings before a court or tribunal.

56 Exemption—eligible data breach of more than 1 agency

(1) This section applies if—

(a) an agency is not required to comply with requirements about assessing a data breach under section 48(2)(b) and (3) because section 48(5) applies to the agency; and

(b) another agency is required to comply with division 2 in relation to the data breach.

(2) The agency need not comply with division 2 in relation to the data breach.

57 Exemption—agency has taken remedial action

(1) This section applies in relation to an eligible data breach of an agency if—

(a) for a data breach involving unauthorised access to, or disclosure of, personal information—

(i) the agency takes action to mitigate the harm caused by the data breach; and

(ii) the action is taken before the access or disclosure results in serious harm to any individual; and

(iii) as a result of the action taken, the data breach is no longer likely to result in serious harm to any individual; or

(b) for a data breach involving the loss of personal information—

(i) the agency takes action to mitigate the loss; and

(ii) the action is taken before there is unauthorised access to, or disclosure of, the personal information; and

(iii) as a result of the action taken, there is no unauthorised access to, or disclosure of, the personal information; or

(c) for a data breach involving the loss of personal information—

(i) the agency takes action to mitigate the loss; and

(ii) the action is taken after there is unauthorised access to, or unauthorised disclosure of, the personal information but before the access or disclosure results in serious harm to any individual; and

(iii) as a result of the action taken, the data breach is no longer likely to result in serious harm to any individual.

(2) The agency need not comply with section 53 in relation to the eligible data breach.

58 Exemption—inconsistency with confidentiality provision

An agency need not comply with division 2 in relation to an eligible data breach of the agency to the extent the compliance would be inconsistent with a provision of an Act of the Commonwealth or a State that prohibits or regulates the use or disclosure of the information.

59 Exemption—serious risk of harm to health or safety

(1) An agency need not comply with section 53 in relation to an eligible data breach to the extent compliance would create a serious risk of harm to an individual's health or safety, having regard to, for example—

(a) whether the harm caused by complying with division 2 is greater than the harm of not complying with that division; and

(b) the currency of the information relied on.

(2) If an agency relies on this section, the agency must give a written notice to the information commissioner stating—

(a) the extent to which the agency is exempt from complying with division 2 under this section; and

(b) whether or not the exemption is permanent or temporary; and

(c) if the exemption is temporary—when the agency expects the exemption will stop applying.

60 Exemption—compromise to cybersecurity

(1) An agency need not comply with section 53 in relation to an eligible data breach if compliance is likely to—

(a) compromise or worsen the agency's cybersecurity; or

(b) lead to further data breaches of the agency.

(2) The exemption applies only for the period during which a matter mentioned in subsection (1)(a) or (b) continues to apply for the agency in relation to the eligible data breach.

(3) If an agency relies on this section, the agency must give a written notice to the information commissioner stating—

(a) the agency is exempt from complying with division 2 under this section; and

(b) when the agency expects the exemption will stop applying; and

(c) how the agency will review the application of the exemption.

(4) The agency must—

(a) review the application of the exemption each month for the period during which the exemption is relied on; and

(b) give the commissioner a summary of the review as soon as practicable after it is completed.

Part 4 Role of information commissioner

61 Information commissioner may direct agency to give statement and make recommendations

(1) This section applies if the information commissioner reasonably suspects a data breach of an agency may be an eligible data breach of the agency.

(2) The information commissioner may, after complying with subsections (5) and (6), direct the agency by written notice to prepare and give to the commissioner a statement providing the following information—

(a) the name and contact details of the agency and, if more than 1 agency was affected by the data breach, the name of each other agency;

(b) a description of the data breach, including the kind of personal information involved in the data breach;

(c) recommendations about the steps an individual who may be affected by the data breach should take in response to the data breach;

(d) any other information related to the data breach requested by the commissioner.

(3) The agency must comply with the direction.

(4) If a direction is given under subsection (2), the information commissioner may also, after complying with subsections (5) and (6), recommend to the agency that the agency notify individuals under section 53 as if the agency reasonably believed the data breach were an eligible data breach.

(5) Before giving a direction under subsection (2) or making a recommendation under subsection (4), the information commissioner must invite the agency to make a submission to the commissioner, within a reasonable period, about the data breach.

(6) Without limiting the matters the information commissioner may consider, in deciding whether to give a direction under subsection (2) or make a recommendation under subsection (4), the information commissioner must have regard to the following—

(a) any advice given to the information commissioner by a law enforcement agency;

(b) any submission made by the agency under subsection (5).

Part 5 Investigations

Division 1 Authorised officers

62 Functions

The functions of an authorised officer are to monitor and investigate whether an occasion has arisen for the exercise of the information commissioner's powers that relate to an agency's compliance with this chapter.

63 Appointment

The information commissioner may, by instrument in writing, appoint an appropriately qualified person as an authorised officer.

64 Identity cards

(1) The information commissioner must issue an identity card to each authorised officer.

(2) The identity card must—

(a) contain a recent photo of the authorised officer; and

(b) contain a copy of the signature of the information commissioner and authorised officer; and

(c) identify the person as an authorised officer under this part; and

(d) state an expiry date for the card.

65 Production or display of identity card

(1) In exercising a power in relation to a person in the person's presence, an authorised officer must—

(a) produce the authorised officer's identity card for the person's inspection before exercising the power; or

(b) have the identity card displayed so it is clearly visible to the person when exercising the power.

(2) However, if it is not practicable to comply with subsection (1), the authorised officer must produce the identity card for the person's inspection at the first reasonable opportunity.

(3) For subsection (1), an authorised officer does not exercise a power in relation to a person only because the authorised officer has entered a place as mentioned in section 67(1)(b).

66 Return of identity card

If the office of a person as an authorised officer ends, the person must return the person's identity card to the information commissioner within 15 business days after the office ends unless the person has a reasonable excuse.

Maximum penalty—10 penalty units.

Division 2 Entry of places occupied by agencies

67 General power to enter places occupied by agency

(1) An authorised officer may enter an agency's place of business, or another place occupied by the agency, if—

(a) the agency has consented to the entry under section 68; or

(b) the place is the agency's place of business and—

(i) is open for carrying on the business; or

(ii) is otherwise open for entry.

(2) However, an authorised officer may enter a place under subsection (1)(a) only if the information commissioner has complied with section 68 before the entry is made.

(3) For subsection (1)(b), a ***place of business*** does not include a part of the place where a person resides.

68 Information commissioner must give written notice of entry

(1) Before an authorised officer enters a place occupied by an agency under section 67(1)(a), the information commissioner must, by written notice, ask the agency to consent to an authorised officer entering the place under section 67(1).

(2) The notice must—

(a) explain the purpose of the entry, including the powers intended to be exercised; and

(b) propose a reasonable date and time for the entry; and

(c) ask for the agency's principal officer's written consent to the entry to be given to the information commissioner within a stated reasonable period; and

(d) if the place is the agency's place of business, state that if the written consent is not given to the commissioner within the stated period, an authorised officer may, under section 67(1)(b), enter the place on a stated reasonable date and at a stated reasonable time.

(3) If the notice is given to an agency, the agency must take all reasonable steps to facilitate entry by an authorised officer on the date and time consented to or stated under subsection (2)(d).

Maximum penalty—100 penalty units.

Division 3 Powers of authorised officers after entering places

69 General powers

If an authorised officer enters a place under section 67(1), the authorised officer may do the following—

(a) require a person at the place who has the necessary skills or knowledge to demonstrate the data handling systems and practices of the agency that relate to the agency's compliance with this chapter;

(b) inspect a document that is relevant to the systems, policies and practices of the agency that relate to the agency's compliance with this chapter;

(c) remain at the place for the time necessary to achieve the purpose of the entry.

70 Power to require reasonable help

(1) If an authorised officer enters a place occupied by an agency under section 67, the authorised officer may require a person at the place to give the authorised officer reasonable help to exercise a power under that section, including, for example, to demonstrate data handling systems and practices or produce a document.

(2) When making a requirement under subsection (1), the authorised officer must give the person an offence warning for the requirement.

(3) In this section—

offence warning, for a requirement made by an authorised officer under subsection (1), means a warning that, without a reasonable excuse, it is an offence for the person of whom the requirement is made not to comply with the requirement.

71 Offence to contravene help requirement

(1) A person of whom a requirement is made under section 70(1) must comply with the requirement unless the person has a reasonable excuse.

Maximum penalty—100 penalty units.

(2) It is a reasonable excuse for an individual not to comply with a requirement under section 70(1) if complying with the requirement might—

(a) tend to incriminate the individual or expose the individual to a penalty; or

(b) result in the disclosure of information that is the subject of legal professional privilege; or

(c) result in the disclosure of confidential information in contravention of a law.

(3) However, subsection (2) does not apply if a document or information the subject of the help requirement is required to be held or kept by the individual under this Act.

Note—

See, however, section 74.

Part 6 Miscellaneous

72 Agency must keep register

(1) An agency must keep a register of eligible data breaches of the agency.

(2) The register must include the following information for each eligible data breach—

(a) a description of the eligible data breach, including the type of data breach under section 47;

(b) if a statement is required for the eligible data breach under section 51—the date the statement is provided;

(c) if further information about the eligible data breach is required to be given to the information commissioner under section 52—each date the further information is given;

(d) if individuals are notified of the eligible data breach under section 53(1)(a) or (b)—the individuals notified and the date and method used to notify the individuals;

(e) if the agency relied on an exemption under part 3, division 3—the exemption relied on;

(f) details of the steps taken by the agency to—

(i) contain the eligible data breach under section 48(2)(a) or (4)(a); and

(ii) mitigate the harm caused by the eligible data breach under section 48(4)(a);

(g) details of the actions taken by the agency to prevent future data breaches of a similar kind occurring.

(3) If it is not practicable to include any or all of the information mentioned in subsection (2) for an eligible data breach at a particular time, the agency must record the information in the register as soon as it is practicable to do so.

73 Agency must publish data breach policy

(1) An agency must prepare and publish a policy about how it will respond to a data breach, including a suspected eligible data breach, of the agency.

(2) The policy must be published on an accessible agency website.

74 Evidential immunity for individuals complying with particular requirements

(1) Subsection (2) applies if an individual gives information to an authorised officer under section 69(1) or 70(1).

(2) Evidence of the information, and other evidence directly or indirectly derived from the information, is not admissible against the individual in any proceeding to the extent it tends to incriminate the individual, or expose the individual to a penalty, in the proceeding.

(3) Subsection (2) does not apply to a proceeding about the false or misleading nature of the information or anything in which the false or misleading nature of the information is relevant evidence.

Chapter 4 Information Commissioner and Privacy Commissioner

Note—

A reference in this chapter to an agency includes a reference to a Minister, a department, a local government or a public authority—see section 18.

Part 1 Functions of information commissioner under this Act

134 Information commissioner not subject to direction

(1) The information commissioner is not subject to direction by any person about—

(a) the way in which the commissioner's powers are to be exercised in the performance of a function under section 135 or 136; or

(b) the priority to be given to investigations, reviews, audits mentioned in section 135(1)(b)(iii) and privacy complaints under this Act.

(2) Subsection (1) has effect despite the *Public Sector Act 2022*.

135 Performance monitoring, investigation and support functions

(1) The functions of the information commissioner include—

(a) on the commissioner's own initiative or otherwise—

(i) conducting reviews into personal information handling practices of relevant entities, including technologies, programs, policies and procedures, to identify privacy related issues of a systemic nature generally or to identify particular grounds for the issue of compliance notices; and

(ii) investigating an act done or practice engaged in by a relevant entity in relation to personal information, if the commissioner is satisfied on reasonable grounds that the act or practice may contravene the privacy principle requirements or, if the entity is an agency, the entity's obligations under chapter 3A; and

(b) leading the improvement of public sector privacy administration in Queensland by taking appropriate action to—

(i) promote understanding of and compliance with the privacy principle requirements; and

(ii) provide best practice leadership and advice, including by providing advice and assistance to relevant entities on the interpretation and administration of this Act; and

(iii) monitor and audit relevant entities' compliance with this Act; and

(iv) initiate privacy education and training, including education and training programs targeted at particular aspects of privacy administration, and education and training programs to promote greater awareness of the operation of this Act in the community and within the public sector environment; and

(v) comment on any issues relating to the administration of privacy in the public sector environment; and

(vi) without limiting subparagraph (v), identify and comment on legislative and administrative changes that would improve the administration of this Act; and

(vii) prepare, or assist in the preparation of, QPP codes; and

(viii) assist relevant entities in complying with obligations under QPP codes; and

(ix) prepare guidelines for permitted general situations under chapter 3, part 2; and

(c) issuing guidelines under section 138; and

(d) supporting complainants for privacy complaints, and all relevant entities to the extent they are subject to the operation of this Act; and

(e) if the commissioner considers it appropriate, reporting to the Speaker on the findings of a reportable matter, including reporting any recommendations to the relevant entity the subject of the reportable matter.

(2) In this section—

reportable matter means—

(a) a review or investigation under subsection (1)(a); or

(b) an audit under subsection (1)(b)(iii).

136 Decision-making functions

The functions of the information commissioner include—

(a) waiving or modifying—

(i) an obligation of an agency to comply with the privacy principle requirements; or

(ii) an obligation of an agency to comply with chapter 3A, part 2 or 3 or section 72 or 73; and

(b) issuing compliance notices under part 6; and

(c) dealing with privacy complaints under chapter 5.

138 Power to issue guidelines

(1) The information commissioner may issue a guideline about any matter relating to the information commissioner's functions, including, for example, guidelines about—

(a) the interpretation and administration of this Act; and

(b) best practice for relevant entities in relation to information privacy generally; and

(c) the application of the privacy principle requirements, including the factors to be considered in determining whether the QPPs are being complied with.

(2) To remove any doubt, it is declared that—

(a) this section does not limit the information commissioner's power to make guidelines under the Right to Information Act, section 132; and

(b) a guideline issued under that Act may include guidelines relating to the information commissioner's functions under this Act.

Part 2 Staff of Office of Information Commissioner in relation to this Act

139 Delegation

The information commissioner may delegate to a member of the staff of the OIC all or any of the commissioner's powers under this Act.

140 Staff subject only to direction of information commissioner

(1) The staff of the OIC are not subject to direction by any person, other than the information commissioner or a person authorised by the commissioner, about the performance of the commissioner's functions under this Act.

(2) Subsection (1) has effect despite the *Public Sector Act 2022*.

Part 3 Privacy Commissioner

141 The Privacy Commissioner

(1) There is to be a Privacy Commissioner (the ***privacy commissioner***).

(2) The privacy commissioner is a member of the staff of the OIC.

142 Role and function of privacy commissioner

(1) The privacy commissioner's role is that of a deputy to the information commissioner, with particular responsibility for matters relating to the information commissioner's functions under this Act.

(2) The privacy commissioner's function is to perform the functions of the information commissioner under this Act to the extent the functions are delegated to the privacy commissioner by the information commissioner.

143 Privacy commissioner subject to direction of information commissioner

The privacy commissioner is subject to the direction of the information commissioner.

144 Appointment

(1) The privacy commissioner is appointed by the Governor in Council.

(2) The privacy commissioner is appointed under this Act and not under the *Public Sector Act 2022*.

145 Procedure before appointment

(1) A person may be appointed as privacy commissioner only if—

(a) the Minister has placed press advertisements nationally calling for applications from suitably qualified persons to be considered for appointment; and

(b) the Minister has consulted with the parliamentary committee about—

(i) the process of selection for appointment; and

(ii) the appointment of the person as privacy commissioner.

(2) Subsection (1)(a) and (b)(i) does not apply to the reappointment of a person as privacy commissioner.

146 Term of appointment

(1) The privacy commissioner holds office for the term, of not more than 5 years, stated in the instrument of appointment.

(2) However, a person being reappointed as privacy commissioner can not be reappointed for a term that would result in the person holding office as privacy commissioner for more than 10 years continuously.

147 Remuneration and conditions

(1) The privacy commissioner must be paid remuneration and other allowances decided by the Governor in Council.

(2) The remuneration paid to the privacy commissioner must not be reduced during the commissioner's term of office without the commissioner's written agreement.

(3) In relation to matters not provided for by this Act, the privacy commissioner holds office on the terms and conditions decided by the Governor in Council.

148 Leave of absence

The information commissioner may approve a leave of absence for the privacy commissioner in accordance with entitlements available to the privacy commissioner under the privacy commissioner's conditions of office.

149 Preservation of rights if public service officer appointed

(1) A public service officer who is appointed to the office of privacy commissioner or who is appointed to act in the office is entitled to retain all existing and accruing rights as if service in the office were a continuation of service as a public service officer.

(2) If the person stops holding the office for a reason other than misconduct, the person is entitled to be employed as a public service officer.

(3) The person must be employed on the classification level and remuneration that the Public Sector Commission under the *Public Sector Act 2022* or another entity prescribed under a regulation considers the person would have attained in the ordinary course of progression if the person had continued in employment as a public service officer.

150 Restriction on outside employment

(1) The privacy commissioner must not, without the Minister's prior approval in each particular case—

(a) hold any office of profit other than that of privacy commissioner; or

(b) engage in any remunerative employment or undertaking outside the duties of the office.

(2) Contravention of subsection (1) is misconduct under the Right to Information Act, section 160(a).

151 Resignation

(1) The privacy commissioner may resign by signed notice given to the Minister.

(2) As soon as practicable after the notice is given to the Minister, the Minister must—

(a) give the notice to the Governor for information; and

(b) give a copy of the notice to—

(i) the Speaker of the Assembly; and

(ii) the chairperson of the parliamentary committee.

(3) Failure to comply with subsection (2) does not affect the effectiveness of the resignation.

152 Acting privacy commissioner

(1) The Governor in Council may appoint a person to act as privacy commissioner—

(a) during a vacancy in the office; or

(b) during any period, or during all periods, when the privacy commissioner is absent from duty or from Australia or is, for another reason, unable to perform the duties of the office.

(2) The acting privacy commissioner is appointed under this Act and not the *Public Sector Act 2022*.

(3) The *Acts Interpretation Act 1954*, section 25(1)(b)(iv) and (v) does not apply to the office of acting privacy commissioner.

Part 4 Proceedings

153 Third party proceedings

(1) The information commissioner or a member of the staff of the OIC can not be compelled—

(a) to produce a privacy document in third party legal proceedings; or

(b) to disclose privacy information in third party legal proceedings.

(2) In this section—

privacy document means a document received, or created, by the commissioner or member in performing functions under this Act.

privacy information means information that the commissioner or member obtained in performing functions under this Act.

third party legal proceedings means a legal proceeding other than—

(a) a legal proceeding started by the commissioner; or

(b) a legal proceeding started against the commissioner or member arising out of the performance of functions under this Act.

154 Costs in proceedings

If a proceeding arising out of the performance of the functions of the information commissioner under this Act is started by the State, the reasonable costs of a party to the proceeding must be paid by the State.

155 Information commissioner and privacy commissioner may appear in proceedings

The information commissioner or privacy commissioner is entitled to appear and be heard in a proceeding arising out of the performance of the functions of the commissioner.

156 Intervention by Attorney-General

(1) The Attorney-General may, for the State, intervene in a proceeding before a court arising out of the performance of the functions of the information commissioner under this Act.

(2) If the Attorney-General intervenes—

(a) the court may make the order as to costs against the State the court considers appropriate; and

(b) the Attorney-General becomes a party to the proceeding.

Part 5 Waiving or modifying particular obligations in the public interest

157 Applying for waiver or modification of particular obligations

(1) A relevant entity may apply to the information commissioner for an approval that waives or modifies an obligation of the entity to comply with—

(a) the privacy principle requirements; or

(b) for an agency—chapter 3A, part 2 or 3 or section 72 or 73.

(2) The commissioner may, by gazette notice, give an approval that waives or modifies an obligation mentioned in subsection (1)—

(a) if it is a temporary approval—for the period of the approval's operation; or

(b) otherwise—until the approval is revoked or amended.

(3) The *Statutory Instruments Act 1992*, sections 49 to 51 apply to a gazette notice under subsection (2), including a gazette notice revoking or amending an approval, as if it were subordinate legislation.

(4) The commissioner may give an approval under this section for an obligation only if the commissioner is satisfied that the public interest in the relevant entity's compliance with the obligation is outweighed by the public interest in waiving or modifying the entity's compliance with the obligation to the extent stated in the approval.

(5) While an approval is in force, the relevant entity does not contravene this Act in relation to the obligation the subject of the approval if the entity acts in accordance with the approval.

(6) If the commissioner gives an approval under this section—

(a) the commissioner must also ensure that a copy of the gazette notice is published on the commissioner's website on the internet while the approval is in force; and

(b) if it is practicable to do so, the agency the subject of the approval must ensure that a copy of the gazette notice is published on the agency's website on the internet.

Part 6 Compliance notices

158 Compliance notice

(1) The information commissioner may give a relevant entity a notice (a ***compliance notice***) if the commissioner is satisfied on reasonable grounds that the entity—

(a) has done an act or engaged in a practice in contravention of a relevant obligation; and

(b) the act or practice—

(i) is a serious or flagrant contravention of the obligation; or

(ii) is of a kind that has been done or engaged in by the agency on at least 5 separate occasions within the last 2 years.

(2) A compliance notice may require a relevant entity to take stated action within a stated period for the purpose of ensuring compliance with the obligation.

(3) In this section—

relevant obligation means an obligation to comply with—

(a) the privacy principle requirements; or

(a) for an agency—

(i) chapter 3A, part 2 or 3; or

(ii) a direction given to the agency under section 61(2); or

(iii) section 72 or 73.

159 Extension of time for compliance

(1) A relevant entity that is given a compliance notice may ask the information commissioner to extend the time within which it must take the action stated in the compliance notice.

(2) The commissioner may amend the compliance notice by extending the period stated in the compliance notice for taking the action stated in the notice.

(3) Before the commissioner extends the period—

(a) the commissioner must be satisfied that it is not reasonably practicable for the relevant entity to take the action stated in the compliance notice within the time stated in the notice; and

(b) the relevant entity must give the commissioner an undertaking to take the stated action within the extended period.

160 Relevant entity must comply with notice

A relevant entity that is given a compliance notice under this part must take all reasonable steps to comply with the notice.

Maximum penalty—100 penalty units.

161 Application to Queensland Civil and Administrative Tribunal for review of decision to give compliance notice

(1) A relevant entity given a compliance notice under this part may apply, as provided under the QCAT Act, to QCAT for a review of a decision of the information commissioner to give the entity the compliance notice.

(2) QCAT must exercise its review jurisdiction under the QCAT Act.

162 Parties to QCAT proceeding

The relevant entity given a compliance notice under this part and the information commissioner are both parties to—

(a) an application to QCAT to review the decision to give the notice; and

(b) any review by QCAT of the decision.

163 How QCAT may dispose of review

If QCAT reviews a decision of the information commissioner to give a relevant entity a compliance notice, QCAT may make any of the following orders—

(a) confirm the commissioner's decision to give the compliance notice;

(b) confirm the commissioner's decision to give a compliance notice but substitute a compliance notice that is in different terms from the compliance notice given;

(c) revoke the giving of the compliance notice;

(d) revoke the giving of the compliance notice and give the commissioner directions about the issuing of a replacement compliance notice.

Chapter 5 Privacy complaints

Note—

A reference in this chapter to an agency includes a reference to a Minister, a department, a local government or a public authority—see section 18.

Part 1 Making privacy complaints

164 Meaning of *privacy complaint*

(1) A ***privacy complaint*** is a complaint by an individual about an act done or practice engaged in by a relevant entity in relation to the individual's personal information that may be a breach of the relevant entity's obligation to comply with—

(a) the privacy principle requirements; or

(b) for an agency—chapter 3A, part 2 or 3.

(2) However, a ***privacy complaint*** does not include a complaint in relation to the individual's personal information to the extent the personal information is—

(a) in a document to which this Act does not apply; or

(b) if the personal information is held by a bound contracted service provider—in a document held by the provider other than for the purpose of performing its obligations under the provider's service arrangement.

164A Response period for privacy complaints

(1) The ***response period*** for a privacy complaint made to a relevant entity is—

(a) the period of 45 business days after the day the privacy complaint is received by the relevant entity; or

(b) if the relevant entity asks the complainant for a longer period under subsection (2)—the period during which, under subsection (4), the relevant entity may continue to consider the privacy complaint, in addition to the period mentioned in paragraph (a).

(2) The relevant entity may, before the end of a response period under subsection (1), ask the complainant for a further specified period to consider the complaint.

(3) A request under subsection (2) may be made more than once.

(4) If the relevant entity makes a request under subsection (2), the relevant entity may continue to consider the complaint and respond to it until—

(a) the complainant refuses the request; or

(b) the relevant entity receives a notice that the complainant has made a privacy complaint to the information commission; or

(c) the further specified period requested under subsection (2) ends.

165 Privacy complaint may be made or referred to information commissioner

(1) An individual whose personal information is, or at any time has been, held by a relevant entity may make a privacy complaint to the information commissioner.

(2) Also, a privacy complaint may be referred to the commissioner by any of the following entities—

(a) the ombudsman;

(b) the health ombudsman under the *Health Ombudsman Act 2013*;

(c) the human rights commissioner under the *Anti-Discrimination Act 1991*;

(d) a person or other entity having responsibilities, under a law of another State or the Commonwealth that corresponds to this Act, that correspond to the responsibilities of the commissioner under this Act;

(e) any other commission or external review body that has received the privacy complaint in performing its functions under a law.

(3) As soon as practicable after receiving a privacy complaint made or referred under this section, the commissioner must advise the relevant entity the subject of the complaint.

166 Requirements for privacy complaint to information commissioner

(1) A privacy complaint made or referred to the information commissioner must—

(a) be written; and

(b) state an address of the complainant to which notices may be forwarded under this Act; and

(c) give particulars of the act or practice the subject of the complaint.

(2) For a privacy complaint made to the commissioner by an individual, the commissioner must give reasonable help to the complainant to put the complaint into written form.

(3) However, an individual may not make a privacy complaint to the commissioner unless—

(a) the individual has first made a privacy complaint to the relevant entity under section 166A; and

(b) either—

(i) the individual does not consider the relevant entity's response to the complaint to be adequate; or

(ii) the response period for the complaint has ended and the individual has not received a response to the complaint.

166A Requirements for privacy complaint to relevant entity

(1) A privacy complaint made to a relevant entity by an individual must—

(a) be in writing; and

(b) state an address to which the entity may respond to the complaint; and

(c) give particulars of the act or practice the subject of the complaint; and

(d) be made within 12 months after the complainant becomes aware of the act or practice the subject of the complaint, or a longer period agreed by the relevant entity.

(2) The relevant entity may agree to a longer period under subsection (1)(d) if the relevant entity is satisfied the extension is reasonable in the circumstances.

(3) The relevant entity must give reasonable help to the individual to put the complaint in writing.

Part 2 Dealing with privacy complaints

167 Preliminary action

The information commissioner may make preliminary inquiries of the complainant and the respondent for a privacy complaint to decide whether the commissioner is authorised to deal with the privacy complaint and whether the commissioner may decline to deal with the complaint.

168 Information commissioner may decline to deal with or to deal further with complaint

(1) The information commissioner may decline to deal with a privacy complaint, or a part of a privacy complaint, made or referred to the commissioner if—

(a) the act or practice the subject of the complaint or part does not relate to the personal information of the complainant; or

(b) the requirements under section 166(3) for making a complaint have not been fully satisfied; or

(c) the commissioner reasonably believes the complaint or part is frivolous, vexatious, misconceived or lacking in substance; or

(d) there is a more appropriate course of action available under another Act to deal with the substance of the complaint or part; or

(e) although the complainant made the complaint to the respondent as required under section 166(3), in the circumstances, the respondent has not yet had an adequate opportunity to deal with the complaint or part; or

(f) 12 months have elapsed since the earlier of the following days—

(i) the last day of the response period for the complaint;

(ii) the day the relevant entity responds to the complaint or part.

(2) The commissioner may decline to continue dealing with a privacy complaint, or a part of a privacy complaint, made or referred to the commissioner if—

(a) the complainant does not comply with a reasonable request made by the commissioner in dealing with the complaint or part; or

(b) the commissioner is satisfied on reasonable grounds that the complainant, without a reasonable excuse, has not cooperated in the commissioner's dealing with the complaint or part; or

(c) the commissioner considers the address the complainant stated in making the privacy complaint is no longer the address at which the complainant can be contacted, and the complainant has not, within a reasonable time, advised the commissioner of a new address to which notices may be sent under this Act.

169 Referral of privacy complaint to other entity

(1) If the subject of a privacy complaint could be the subject of a complaint under the *Ombudsman Act 2001*, the information commissioner may refer the complaint to the ombudsman.

(2) If the subject of a privacy complaint could be the subject of a complaint under the *Health Ombudsman Act 2013*, the commissioner may refer the complaint to the health ombudsman under that Act.

(3) If the subject of a privacy complaint could be the subject of a complaint under a law of another State or the Commonwealth that corresponds to this Act, the commissioner may refer the complaint to the entity under that law having responsibility for dealing with complaints in the nature of privacy complaints.

170 Arrangement with ombudsman

(1) The information commissioner may enter into an arrangement with the ombudsman providing for—

(a) the privacy complaints under this chapter that the commissioner should refer to the ombudsman because they—

(i) relate to administrative actions; and

(ii) would be more appropriately dealt with by the ombudsman under the *Ombudsman Act 2001*; or

(b) the complaints under the *Ombudsman Act 2001* that the ombudsman should refer to the commissioner because they—

(i) relate to decisions or other actions for which the commissioner has jurisdiction; and

(ii) would be more appropriately dealt with by the commissioner under this chapter; or

(c) how to deal with an administrative action that is the subject of a complaint, preliminary inquiry or investigation under the *Ombudsman Act 2001* and a privacy complaint under this chapter; or

(d) the cooperative performance by the commissioner and the ombudsman of their respective functions relating to administrative actions.

(2) If an arrangement entered into under subsection (1) provides for referrals as mentioned in subsection (1)(a) or (b), the arrangement must also provide for how the referral is to be made.

(3) The commissioner and the ombudsman are empowered to perform their functions in accordance with any relevant arrangement entered into under this section.

(4) In this section—

administrative action has the meaning given by the *Ombudsman Act 2001*, section 7.

Part 3 Mediation of privacy complaints

171 Attempting resolution through mediation

(1) The information commissioner must consider whether, in the circumstances as known to the commissioner, resolution of a privacy complaint could be achieved through mediation.

(2) If it appears to the commissioner that it is reasonably likely that resolution of the privacy complaint could be achieved through mediation, the commissioner must take all reasonable steps to cause the complaint to be mediated.

172 Certification of mediated agreement

(1) This section applies if, after mediation of a privacy complaint, the complainant and the respondent for the complaint agree on a resolution of the complaint.

(2) The complainant or the respondent may ask the information commissioner to prepare a written record of the agreement.

(3) A request under subsection (2) must be made within 20 business days after the agreement is reached under subsection (1).

(4) If a request is made under subsection (2), the commissioner must take all reasonable steps to—

(a) prepare a written record of the agreement; and

(b) have the record signed by both the complainant and the respondent; and

(c) certify the agreement.

173 Filing of certified agreement with Queensland Civil and Administrative Tribunal

(1) The complainant or respondent to a privacy complaint the subject of a certified agreement under this part may file a copy of the agreement with QCAT.

(2) QCAT may make orders necessary to give effect to the certified agreement if, within 5 business days after the agreement is filed with QCAT, neither the complainant nor the respondent advises QCAT that the party wishes to withdraw from the agreement.

(3) However, QCAT may make an order under subsection (2) only if it is satisfied that implementation of the order is practicable and that the order is consistent with an order QCAT may make under the QCAT Act.

(4) An order under subsection (2) becomes, and may be enforced as, an order of QCAT under the QCAT Act.

173A Confidentiality of mediation

Nothing said or done in the course of a mediation of a privacy complaint is admissible in any criminal, civil or administrative proceeding, unless the complainant and respondent for the complaint agree.

Part 4 Referral of privacy complaints to QCAT

174 Application of pt 4

This part applies if a privacy complaint is made to the information commissioner under this chapter, and—

(a) it does not appear to the commissioner reasonably likely that resolution of the complaint could be achieved through mediation; or

(b) mediation of the complaint is attempted under this chapter but a certified agreement for the resolution of the complaint is not achieved.

175 Advice to parties

The information commissioner must give written notice to both the complainant and the respondent for the privacy complaint advising—

(a) that this part applies and why it applies; and

(b) that the complainant may ask the commissioner to refer the privacy complaint to QCAT under section 175A.

175A Complainant's request for referral to Queensland Civil and Administrative Tribunal

(1) Within 20 business days after the date of the notice given under section 175, the complainant may, by written notice given to the information commissioner, ask the commissioner to refer the privacy complaint to QCAT.

(2) The information commissioner may, if asked by the complainant, extend the period mentioned in subsection (1) if the commissioner is satisfied extending the period is reasonable in all the circumstances.

(3) If the information commissioner extends the period under subsection (2), the commissioner must give a written notice to the complainant and the respondent for the privacy complaint stating the new period within which the complainant may give notice under subsection (1).

176 Referral to Queensland Civil and Administrative Tribunal

(1) If the complainant gives written notice to the information commissioner under section 175A, the commissioner must refer the privacy complaint to QCAT within 20 business days after receiving the written notice.

(2) QCAT must exercise its original jurisdiction under the QCAT Act to hear and decide a privacy complaint referred to it under this section.

177 Parties to QCAT proceeding

(1) The complainant and respondent for a privacy complaint the information commissioner refers to QCAT are both parties to the proceeding before QCAT.

(2) The complainant is taken to be the applicant for the proceeding before QCAT.

178 How QCAT may dispose of complaint

After the hearing of a privacy complaint referred to QCAT, QCAT may make 1 or more of the following orders—

(a) an order that the breach the subject of the complaint, or part of the complaint, has been substantiated, together with, if considered appropriate, an order in accordance with 1 or more of the following—

(i) that the respondent must not repeat or continue the act or practice the subject of the complaint;

(ii) that the respondent must engage in a stated reasonable act or practice to compensate for loss or damage suffered by the complainant;

(iii) that the respondent must apologise to the complainant for the act or practice the subject of the complaint;

(iv) that the respondent must make stated amendments of documents it holds;

(v) that the respondent is liable to pay the complainant a stated amount, of not more than $100,000 to compensate the complainant for loss or damage suffered by the complainant because of the act or practice the subject of the complaint, including for

any injury to the complainant's feelings or humiliation suffered by the complainant;

(b) an order that the breach the subject of the complaint, or part of the complaint, has been substantiated together with an order that no further action is required to be taken;

(c) an order that the breach the subject of the complaint, or part of the complaint, has not been substantiated, together with an order that the complaint or part is dismissed;

(d) an order that the complainant be reimbursed for expenses reasonably incurred in connection with making the complaint.

Chapter 6 Protections and offences

Part 1 Protections

179 Access—protection against actions for defamation or breach of confidence

(1) If a person has been given access to a document and the access was required or permitted to be given under this Act—

(a) no action for defamation or breach of confidence lies against the State, an agency or an officer of an agency because of the authorising or giving of the access; and

(b) no action for defamation or breach of confidence in relation to any publication involved in, or resulting from, the giving of the access lies against the author of the document or another person because of the author or another person having given the document to an agency.

(2) The giving of access to a document in compliance with the privacy principle requirements must not be taken for the

purposes of the law relating to defamation or breach of confidence to constitute an authorisation or approval of the publication of the document or its contents by the person to whom access is given.

181 Access—protection in respect of offences

If access has been given to a document and the access was required or permitted to be given under this Act, neither the person authorising the access nor any other person concerned in the giving of the access commits a criminal offence merely because of the authorising or giving of the access.

183 Protection of agency, information commissioner etc. from personal liability

(1) A relevant entity does not incur civil liability for an act done or omission made honestly and without negligence under this Act.

(2) A liability that would, other than for this section, attach to a relevant entity attaches instead to the State.

(3) In this section—

relevant entity means any of the following—

(a) an agency;

(b) an agency's principal officer;

(c) a person acting under the direction of an agency or an agency's principal officer;

(d) the information commissioner;

(e) a member of the staff of the OIC.

Part 2 Offences

184 Direction to act in particular way

(1) A person must not give a direction, either orally or in writing to a person required or permitted to make a decision under this Act directing the person to make a decision the person believes is not the decision that should be made under this Act.

Maximum penalty—100 penalty units.

(2) Subsection (1) does not apply to the information commissioner or a person authorised by the commissioner in relation to a direction that may be given to a member of the staff of the OIC under section 140.

(3) A person must not give a direction, either orally or in writing to a person who is an employee or officer of the agency involved in a matter under this Act directing the person to act contrary to the requirements of this Act.

Maximum penalty—100 penalty units.

185 Unlawful access

A person must not, in order to gain access to a document containing another person's personal information, knowingly deceive or mislead a person exercising powers under this Act.

Maximum penalty—100 penalty units.

186 False or misleading information

(1) A person must not give information to an official that the person knows is false or misleading in a material particular.

Maximum penalty—100 penalty units.

(2) Subsection (1) does not apply to information given in a document, if the person when giving the document—

(a) informs the official, to the best of the person's ability, how the information is false or misleading; and

(b) gives the correct information to the official if the person has, or can reasonably obtain, the correct information.

(3) It is enough for a complaint against a person for an offence against subsection (1) to state that the information was 'false or misleading', without specifying whether it was false or whether it was misleading.

(4) In this section—

official means—

(a) the information commissioner; or

(b) a member of the staff of the OIC; or

(c) an authorised officer.

187 Failure to give information or attend proceedings

(1) A person given notice under section 197 to give information to, or attend before, the information commissioner must not, without reasonable excuse, fail to do so.

Maximum penalty—100 penalty units.

(2) If the person is an individual and is given notice to give information, it is a reasonable excuse for the person to fail to give the information if complying with the requirement might tend to incriminate the person or expose the person to a penalty.

(3) Subsection (2) does not apply in relation to information that is in a document required to be kept by the person under this Act.

188 Disclosure or taking advantage of information

(1) If a person is or has been the information commissioner or a member of the staff of the OIC, the person must not—

(a) otherwise than for the purposes of this Act or a proceeding arising under this Act, disclose any information that the person obtained in performing functions under this Act; or

(b) take advantage of that information to benefit themself or another person.

Maximum penalty—100 penalty units.

(2) Subsection (1)(a) does not apply if the person reasonably believes that the disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual, or to public health or safety.

Chapter 7 Miscellaneous provisions

Note—

A reference in this chapter to an agency includes a reference to a Minister, a department, a local government or a public authority—see section 18.

Part 2 Operation of this Act

192 Review of Act

(1) The Minister must review this Act and the review must start no later than 2 years after the commencement of this section.

(2) The objects of the review include—

(a) deciding whether the primary object of this Act remains valid; and

(b) deciding whether this Act is meeting its primary object; and

(c) deciding whether the provisions of this Act are appropriate for meeting its primary object; and

(d) investigating any specific issue recommended by the Minister or the information commissioner.

(3) The Minister must, as soon as practicable after finishing the review, table a report about the outcome of the review in the Assembly.

193 Reports of information commissioner

(1) The information commissioner may make a report to the Speaker on matters relating to—

(a) the findings of a reportable matter under section 135(2); or

(b) the performance of any other function of the commissioner.

(2) The commissioner must, as soon as practicable after the end of each financial year, give the Speaker and parliamentary committee a report of the operations of the OIC under this Act during that year.

(3) A report under subsection (2) must include, in relation to the financial year to which it relates, details of the matters prescribed under a regulation.

(4) The parliamentary committee may require the information commissioner to prepare and give the committee a report on a particular aspect of the performance of the commissioner's functions.

(5) If a report of the commissioner is given to the Speaker or the parliamentary committee, the Speaker or chairperson of the committee must cause the report to be tabled in the Assembly on the next sitting day after it is given.

(6) An annual report under this section may be included as part of an annual report the commissioner is required to give under the Right to Information Act.

194 Report to Assembly on Act's operation

(1) An agency or Minister must, as soon as practicable after the end of each financial year, give the information commissioner the information prescribed by regulation about the operation of this Act in relation to the agency or Minister during that year.

(2) The information commissioner must, as soon as practicable after receiving the information mentioned in subsection (1), prepare a report on the operation of this Act during that year and give the report to the parliamentary committee.

(3) A report under subsection (2) must include, in relation to the financial year to which it relates, details of the matters prescribed by regulation.

(4) The chair of the parliamentary committee must table a report received under subsection (2) in the Assembly within 3 sitting days after the committee receives the report.

(5) A report under this section may be included as part of a report prepared by the information commissioner and given and tabled under the Right to Information Act, section 185.

195 Functions of parliamentary committee

The parliamentary committee has the following functions under this Act—

(a) to monitor and review the performance by the information commissioner of the commissioner's functions under this Act;

(b) to report to the Assembly on any matter concerning the commissioner, the commissioner's functions or the performance of the commissioner's functions that the committee considers should be drawn to the Assembly's attention;

(c) to examine each annual report tabled in the Assembly under this Act and, if appropriate, to comment on any aspect of the report and to make recommendations;

(d) to report to the Assembly any changes to the functions, structures and procedures of the OIC the committee considers desirable for the more effective operation of this Act;

(e) the other functions conferred on the parliamentary committee by this Act.

Part 3 Other

196 Power of person acting for another person

(1) To remove any doubt, it is declared that, in relation to a matter under this Act—

(a) a person's agent is able to do, in accordance with the terms of the person's authorisation as agent, anything that the person could do; and

(b) a child's parent is able to do anything that the child could do if the child were an adult.

(2) In this section—

child means an individual who is under 18 years.

parent—

1 Parent, of a child, means any of the following persons—

(a) the child's mother;

(b) the child's father;

(c) a person who exercises parental responsibility for the child, including a person who is granted guardianship of the child under the *Child Protection Act 1999* or who otherwise exercises parental responsibility for the child under a decision or order of a federal court or a court of a State.

2 However, a person standing in the place of a parent of a child on a temporary basis is not a parent of the child.

3 A parent of an Aboriginal child includes a person who, under Aboriginal tradition, is regarded as a parent of the child.

4 A parent of a Torres Strait Islander child includes a person who, under Island custom, is regarded as a parent of the child.

196A Information commissioner may make preliminary inquiries

The information commissioner may make preliminary inquiries of any person for the purpose of determining whether to investigate an act or practice on the commissioner's own initiative or otherwise under section 135(1)(a)(ii).

197 Power of information commissioner to require information or attendance

(1) This section applies if the information commissioner is satisfied on reasonable grounds that a person has information relevant to—

(a) a review into personal information handling practices under section 135(1)(a)(i); or

(b) an investigation of an act done or practice engaged in by a relevant entity in relation to personal information under section 135(1)(a)(ii); or

(c) an audit under section 135(1)(b)(iii); or

(d) a decision of the commissioner whether to give an agency a compliance notice under chapter 4; or

(e) preliminary inquiries the commissioner is making of the respondent for a privacy complaint under section 167; or

(f) the mediation of a privacy complaint under chapter 5.

(2) The commissioner may give the person a written notice requiring the person to give the information to the commissioner in written form.

(3) The written notice given by the commissioner must state—

(a) where the information must be given to the commissioner; and

(b) a reasonable time at which, or a reasonable period within which, the information must be given.

(4) The commissioner may also give the person a written notice requiring the person to attend before the commissioner at a reasonable time and place stated in the notice to answer questions relevant to the matter mentioned in subsection (1).

(5) The commissioner may administer an oath or affirmation to a person required under subsection (4) to attend before the commissioner and may examine the person on oath or affirmation.

(6) The oath or affirmation is an oath or affirmation that the answers the person will give will be true.

199 Exchange of information

(1) The information commissioner may enter into an arrangement (an ***information-sharing arrangement***) with a prescribed agency for the purpose of sharing or exchanging information—

(a) held by the information commissioner or the prescribed agency; or

(b) to which the information commissioner or prescribed agency has access.

(2) An information-sharing arrangement may relate only to information that assists—

(a) the information commissioner perform the commissioner's functions under this Act; or

(b) the prescribed agency perform its functions.

(3) Under an information-sharing arrangement, the information commissioner and the prescribed agency are, despite another Act or law, authorised to—

(a) ask for and receive information held by the other party to the arrangement or to which the other party has access; and

(b) disclose information to the other party.

(4) In this section—

prescribed agency—

(a) means a department or administrative unit within a department that has functions related to whole of government cybersecurity management and operations; or

(b) a department or government entity of the State, another State or the Commonwealth that has functions related to protecting the privacy of individuals, whether or not the entity has other functions; or

(c) another department, public authority or government entity of the State, another State or the Commonwealth, prescribed by regulation for this paragraph.

199A Corporations legislation displacement

(1) A regulation may declare a provision of this Act that applies in relation to a prescribed corporation to be a Corporations legislation displacement provision for the purposes of the Corporations Act, section 5G.

(2) A regulation under subsection (1) may be declared to apply in relation to—

(a) the whole of the Corporations legislation or a particular provision of the Corporations legislation; or

(b) all prescribed corporations or a particular prescribed corporation.

(3) In this section—

prescribed corporation means a corporation, within the meaning of the Corporations Act, that is declared under section 21(1)(c) to be a public authority for this Act.

200 Approval of forms

The chief executive may approve forms for use under this Act.

201 Regulation-making power

The Governor in Council may make regulations under this Act.

Chapter 8 Transitional provisions

Part 1 Transitional provisions for Act No. 14 of 2009

202 Delayed application of Act other than ch 3 to local governments

(1) This Act, other than the relevant provisions, does not apply to a local government until 1 year after the commencement of this section.

(2) In this section—

relevant provisions means—

(a) chapter 3; and

(b) the other provisions of this Act to the extent they apply for the purposes of chapter 3.

203 Outdated references

In an Act or document, if the context permits, a reference to the *Freedom of Information Act 1992* is taken to be a reference to this Act.

204 Pre-enactment recruitment process

An appointment of a person as privacy commissioner after the enactment of this Act is not to be taken to be invalid only because action was taken in relation to the filling of the role of privacy commissioner before the enactment.

205 Refusal to deal with application—previous application for same documents

For section 62 or 63, a first application may be an application under the repealed *Freedom of Information Act 1992*.

206 Delayed filing of certified agreement with QCAT

(1) This section applies if—

(a) a privacy complaint becomes the subject of a certified agreement under chapter 5 before QCAT comes into existence; and

(b) the complainant or respondent for the complaint wishes to file a copy of the agreement with QCAT.

(2) The agreement must be filed within 20 business days after QCAT comes into existence.

207 Delayed referral of privacy complaint to QCAT

(1) This section applies if the information commissioner is required under chapter 5 to refer a privacy complaint to QCAT before QCAT comes into existence.

(2) The commissioner must refer the privacy complaint to QCAT within 20 business days after QCAT comes into existence.

208 Delayed application to QCAT

(1) If a person may appeal to the appeal tribunal under section 132 before QCAT comes into existence, the person may appeal to the appeal tribunal within 20 business days after QCAT comes into existence.

(2) If a person may, within a period, apply to QCAT under section 133 before QCAT comes into existence, the person may apply to QCAT within that period after QCAT comes into existence.

209 Privacy complaints to relate to actions after ch 5 commencement

A privacy complaint may be made only about a breach of an entity's obligation happening after the commencement of chapter 5.

210 Continuing application of relevant information standards

(1) This section applies if—

(a) a contract or other arrangement (the ***relevant agreement***) entered into before the commencement, applies, or otherwise refers to, a relevant information standard; and

(b) on or after the commencement, the relevant information standard is repealed, or the application of the standard in Queensland is otherwise ended.

(2) For the purposes of the ongoing operation of the relevant agreement, the relevant information standard, as in force for the purposes of the relevant agreement immediately before the commencement, continues to apply for the purposes of the relevant agreement as if the standard still applied in Queensland in the same way it applied immediately before the commencement.

(3) In this section—

commencement means the commencement of this section.

relevant information standard means an instrument applying in Queensland before the commencement of this section under the name of—

(a) Information Standard No. 42; or

(b) Information Standard No. 42A.

211 Acts and practices authorised before relevant date

(1) The privacy principles do not apply to an entity in relation to an act done or practice engaged in by the entity on or after the relevant date if the act or practice is necessary for the performance of a contract entered into before the relevant date.

(2) In this section—

relevant date means—

(a) for an entity other than a local government—1 July 2009; or

(b) for a local government—1 July 2010.

Note—

Under section 202, this Act (other than particular provisions mentioned in that section) does not apply to a local government until 1 July 2010.

Part 2 Transitional provisions for State Penalties Enforcement and Other Legislation Amendment Act 2009

212 Definition for pt 2

In this part—

relevant period means the period starting on 1 July 2009 and ending immediately before the commencement of this part.

213 Retrospective validation for particular delegations and directions

(1) A delegation, or an amendment of a delegation, made by a principal officer under this Act during the relevant period is taken to be, and always to have been, as valid as if section 50, as in force immediately after the commencement of this part,

had been in force on the day the delegation, or the amendment, was made.

(2) A direction given by a Minister under this Act during the relevant period is taken to be, and always to have been, as valid as if section 51, as in force immediately after the commencement of this part, had been in force on the day the direction was given.

214 Decision under s 69(2) is a reviewable decision

(1) It is declared that a decision made during the relevant period stating the matters mentioned in section 69(2) is, and always has been, a reviewable decision under this Act as if section 69, as in force immediately after the commencement of this part, had been in force on the day the decision was made.

(2) Despite section 96(c) or 101(1)(d), an application for internal review or external review in relation to the decision may be made within 20 business days after the commencement of this part.

(3) If an application for internal review or external review in relation to the decision is made before the commencement of this part, for the purposes of any review, the application is taken to have been made immediately after the commencement of this part.

Part 3 Transitional provisions for Information Privacy and Other Legislation Amendment Act 2023

215 Definitions for part

In this part—

amendment Act means the *Information Privacy and Other Legislation Amendment Act 2023*.

former, for a provision of this Act, means the provision as in force from time to time before the commencement of the provision in which the term is used.

former IP Act means this Act as in force from time to time before the commencement of the provision in which the term is used.

216 Existing bound contracted service providers

(1) This section applies in relation to a contracted service provider that, immediately before the commencement, was a bound contracted service provider required to comply with former chapter 2, part 1 or 2 and part 3 under former section 36.

(2) The requirement to comply with former chapter 2, part 1 or 2 and part 3 continues to apply to the contracted service provider in relation to personal information it holds under the service arrangement.

(3) This Act applies in relation to the contracted service provider as if a reference to the privacy principle requirements were a reference to the requirement to comply with former chapter 2, part 1 or 2 and part 3 under former section 36.

(4) Subsections (2) and (3) do not prevent the contracted service provider and agency agreeing to vary the service arrangement to require the contracted service provider to comply with chapter 2, parts 1 and 2 and section 41.

(5) This section stops applying in relation to the contracted service provider if the service arrangement is varied as mentioned in subsection (4).

217 Existing access and amendment applications

(1) This section applies if an application or purported application under former chapter 3 has been made, but not finalised, before the commencement.

(2) The former IP Act continues to apply in relation to the application or purported application as if the amendment Act had not been enacted.

(3) For subsection (1), an application or purported application under former chapter 3 has not been finalised until—

(a) a decision on the application or purported application has been made or taken to have been made; and

(b) either—

(i) the time for exercising any review rights or appeal rights in relation to the decision has ended without any rights being exercised; or

(ii) any review or appeal in relation to the decision has ended.

Note—

See also the Right to Information Act, section 206Q.

218 Continued protection for giving access to or publishing chapter 3 documents

(1) This section applies in relation to a chapter 3 document accessed or published—

(a) before the commencement; or

(b) under section 217.

(2) Former sections 179 and 181 continue to apply in relation to the authorising or giving of access to a chapter 3 document as if the amendment Act had not been enacted.

(3) Former sections 180 and 182 continue to apply in relation to the publication of a chapter 3 document as if the amendment Act had not been enacted.

(4) In this section—

chapter 3 document means a chapter 3 document within the meaning of the former IP Act.

219 Delayed application of ch 3A to local governments

Chapter 3A does not apply in relation to an agency that is a local government until the day that is 1 year after the commencement.

220 Existing approvals under former s 157

A waiver or modification approval given under former section 157 lapses on the commencement of this section.

221 Existing compliance notices under s 158

(1) This section applies if—

(a) before the commencement, the information commissioner had given an agency a compliance notice under section 158 in relation to the privacy principles as in force before the commencement; and

(b) immediately before the commencement, the time for complying with the notice under this Act had not ended.

(2) The agency must comply with the notice in relation to the privacy principles under the former IP Act as if the amendment Act had not been enacted.

222 Information commissioner may issue compliance notice for failure to comply with former IP Act

(1) This section applies if—

(a) before the commencement, an agency had done an act or engaged in a practice in contravention of a requirement to comply with the privacy principles under the former IP Act; and

(b) immediately before the commencement the information commissioner had not yet given a compliance notice to the agency under section 158 in relation to the act or practice; and

(c) the act or practice also constitutes a contravention of the privacy principle requirements.

(2) The information commissioner may give the agency a compliance notice under section 158 in relation to the act or practice.

223 Privacy complaints about act or practice of relevant entity not yet made before commencement

(1) This section applies if—

(a) before the commencement, a person could have made a privacy complaint under former chapter 5, part 1 about an act or practice engaged in by a relevant entity before the commencement; and

(b) immediately before the commencement, the privacy complaint had not been made.

(2) The privacy complaint may be made under former chapter 5, and former chapter 5 continues to apply in relation to the complaint, as if the amendment Act had not been enacted.

224 Privacy complaints made but not finalised before commencement

(1) This section applies if—

(a) before the commencement, a privacy complaint was made or referred to the information commissioner under former chapter 5, part 1; and

(b) immediately before the commencement, the complaint, or a part of the complaint, had not been finalised.

(2) Former chapter 5 continues to apply in relation to the privacy complaint or part of the privacy complaint as if the amendment Act had not been enacted.

(3) For subsection (1)(b), a privacy complaint or part of a privacy complaint is finalised if—

(a) any of the following apply—

(i) the information commissioner has declined to deal, or continue to deal, with the complaint or part under former section 168;

(ii) the information commissioner has referred the privacy complaint or part to another entity under section 169;

(iii) a mediated agreement has been certified for the privacy complaint or part under section 172;

(iv) QCAT has disposed of the complaint or part under former section 178; and

(b) the time for exercising any review or appeal rights in relation to a matter mentioned in paragraph (a) has ended without any rights being exercised.

225 Continuation of sections 185 and 187 for chapter 3 documents

(1) This section applies in relation to an offence against former section 185 or 187 committed in relation to a chapter 3 document by a person before the commencement.

(2) Without limiting the *Acts Interpretation Act 1954*, section 20, a proceeding for the offence may be continued or started, and the person may be convicted of and punished for the offence, as if the amendment Act, sections 61 and 63 had not commenced.

(3) Subsection (2) applies despite the Criminal Code, section 11.

226 Report to Assembly on Act's operation

(1) This section applies in relation to a financial year ending before the commencement if the report for the financial year has not been tabled in the Assembly under former section 194.

(2) Former section 194 continues to apply in relation to the financial year as if the amendment Act had not been enacted.

(3) Section 194 as in force on the commencement does not apply in relation to the financial year.

Schedule 1 Documents to which the privacy principle requirements do not apply

section 16

1 Covert activity

A document to the extent it contains personal information—

(a) arising out of, or in connection with, a controlled operation or controlled activity under the *Police Powers and Responsibilities Act 2000* or the *Crime and Corruption Act 2001*; or

(b) arising out of, or in connection with, the covert undertaking of an operation, investigation or function of a law enforcement agency; or

(c) obtained under a warrant issued under the *Telecommunications (Interception and Access) Act 1979* (Cwlth).

2 Witness protection

A document to the extent it contains personal information about a person who is included in a witness protection program under the *Witness Protection Act 2000* or who is subject to other witness protection arrangements made under an Act.

3 Disciplinary actions and misconduct

A document to the extent it contains personal information arising out of—

(a) a complaint under the *Police Service Administration Act 1990*, part 7; or

(b) a complaint, or an investigation of corruption, under the *Crime and Corruption Act 2001*.

4 Public interest disclosure

A document to the extent it contains personal information—

(a) contained in a public interest disclosure under the *Public Interest Disclosure Act 2010*; or

(b) that has been collected in an investigation arising out of a public interest disclosure under the *Public Interest Disclosure Act 2010*.

5 Cabinet and Executive Council

A document to the extent it contains personal information that is also the subject of the Right to Information Act, schedule 3, section 1, 2 or 3.

6 Commissions of inquiry

A document to the extent it contains personal information arising out of a commission of inquiry.

7 Other

A document that is—

(a) a generally available publication; or

(b) kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or

(c) a public record in the custody of Queensland State Archives that is not in a restricted access period under that Act; or

(d) a letter, or anything else, while it is being transmitted by post.

Schedule 2 Entities to which the privacy principle requirements do not apply

section 18(4)

Part 1 Entities to which the privacy principle requirements do not apply

1 the Assembly, a member of the Assembly, a committee of the Assembly, a member of a committee of the Assembly, a parliamentary commission of inquiry or a member of a parliamentary commission of inquiry

2 the Parliamentary Judges Commission of Inquiry appointed under the expired *Parliamentary (Judges) Commission of Inquiry Act 1988*

3 a commission of inquiry issued by the Governor in Council, whether before or after the commencement of this schedule

4 a parents and citizens association under the *Education (General Provisions) Act 2006*

5 a grammar school to which the *Grammar Schools Act 2016* applies

6 a government owned corporation or a subsidiary of a government owned corporation

Part 2 Entities to which the privacy principle requirements do not apply in relation to a particular function

1 a court, or the holder of a judicial office or other office connected with a court, in relation to the court's judicial functions

2 a registry or other office of a court, or the staff of a registry or other office of a court in their official capacity, so far as its or their functions relate to the court's judicial function

3 a tribunal in relation to the tribunal's judicial or quasi-judicial functions

4 a tribunal member or the holder of an office connected with a tribunal, in relation to the tribunal's judicial or quasi-judicial functions

5 a registry of a tribunal, or the staff of a registry of a tribunal in their official capacity, so far as its or their functions relate to the tribunal's judicial or quasi-judicial functions

6 a quasi-judicial entity in relation to its quasi-judicial functions

7 a member of, or the holder of an office connected with, a quasi-judicial entity, in relation to the entity's quasi-judicial functions

8 the staff of a quasi-judicial entity in their official capacity, so far as their functions relate to the entity's quasi-judicial functions

Schedule 3 Queensland privacy principles

section 26

Note—

In this schedule—

(a) each QPP is numbered using the provision number of the corresponding APP; and

(b) a reference in an editor's note to an APP followed by a number is a reference to a provision of the *Privacy Act 1988* (Cwlth), schedule 1, having that number; and

(c) editor's notes describe material differences between a particular QPP and the corresponding APP.

Part 1 Consideration of personal information privacy

1 QPP 1—open and transparent management of personal information

1.1 The object of this QPP is to ensure that agencies manage personal information in an open and transparent way.

Compliance with the QPPs etc.

1.2 An agency must take reasonable steps to implement practices, procedures and systems relating to the agency's functions or activities that—

(a) will ensure the agency complies with the QPPs and any QPP code that binds the agency; and

(b) will enable the agency to deal with inquiries and complaints from individuals about the agency's compliance with the QPPs or any QPP code that binds the agency.

QPP privacy policy

1.3 An agency must have a clearly expressed and up-to-date policy (the ***QPP privacy policy***) about the management of personal information by the agency.

1.4 Without limiting QPP 1.3, the QPP privacy policy of the agency must contain the following information—

(a) the kinds of personal information that the agency collects and holds;

(b) how the agency collects and holds personal information;

(c) the purposes for which the agency collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the agency and seek the correction of the information;

(e) how an individual may complain about a breach of the QPPs, or any QPP code that binds the agency, and how the agency will deal with the complaint;

(f) whether the agency is likely to disclose personal information to entities outside Australia;

(g) if the agency is likely to disclose personal information to entities outside of Australia—the countries in which the recipients are likely to be located if it is practicable to state those countries in the policy.

Availability of QPP privacy policy etc.

1.5 An agency must take reasonable steps to make its QPP privacy policy available—

(a) free of charge; and

(b) in an appropriate form.

Example of how agency may make its QPP privacy policy available—

publication on the agency's website

1.6 If a person requests a copy of the QPP privacy policy of an agency in a particular form, the agency must take reasonable steps to give the person a copy in that form.

2 QPP 2—anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an agency in relation to a particular matter.

2.2 QPP 2.1 does not apply if, in relation to the matter—

(a) the agency is required or authorised under an Australian law, or a court or tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the agency to deal with individuals who have not identified themselves or who have used a pseudonym.

Part 2 Collection of personal information

3 QPP 3—collection of solicited personal information

Personal information other than sensitive information

3.1 An agency must not collect personal information, other than sensitive information, unless the information is reasonably necessary for, or directly related to, 1 or more of the agency's functions or activities.

Editor's note—

The equivalent APP includes a provision applying to certain private sector entities (see APP 3.2).

Sensitive information

3.3 An agency must not collect sensitive information about an individual unless—

(a) the individual consents to the collection of the information and the information is reasonably necessary for, or directly related to, 1 or more of the agency's functions or activities; or

Editor's note—

The equivalent APP includes a provision applying to certain private sector entities (see APP 3.3(a)(ii)).

(b) QPP 3.4 applies in relation to the information.

3.4 This QPP applies in relation to sensitive information about an individual if—

(a) the collection of the information is required or authorised under an Australian law or a court or tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the agency; or

Note—

Permitted general situations are stated in schedule 4, part 1.

(c) the agency is a health agency and a permitted health situation exists in relation to the collection of the information by the agency; or

Note—

Permitted health situations are stated in schedule 4, part 2.

(d) the agency is a law enforcement agency and the agency reasonably believes that the collection of the information is reasonably necessary for, or directly related to, 1 or more of the agency's functions or activities.

Editor's note—

The equivalent APP includes a provision applying to—

(a) the Commonwealth Immigration Department (see APP 3.4(d)(i)); and

(b) non-profit organisations (see APP 3.4(e)).

Means of collection

3.5 An agency must collect personal information only by lawful and fair means.

3.6 An agency must collect personal information about an individual only from the individual unless—

(a) either—

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the agency is required or authorised under an Australian law, or a court or tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This QPP applies to the collection of personal information that is solicited by an agency.

4 QPP 4—dealing with unsolicited personal information

4.1 If—

(a) an agency receives personal information; and

(b) the agency did not solicit the information;

the agency must, within a reasonable period after receiving the information, decide whether or not the agency could have collected the information under QPP 3 if the agency had solicited the information.

4.2 The agency may use or disclose the personal information for the purposes of making the decision under QPP 4.1.

4.3 If—

(a) the agency decides the agency could not have collected the personal information; and

(b) the information is not contained in a public record;

the agency must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If QPP 4.3 does not apply in relation to the personal information, QPPs 5 to 13 apply in relation to the information as if the agency had collected the information under QPP 3.

5 QPP 5—notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an agency collects personal information about an individual, the agency must take steps, if any, that are reasonable in the circumstances to—

(a) notify the individual of the matters mentioned in QPP 5.2 that are reasonable in the circumstances; or

(b) otherwise ensure that the individual is aware of those matters.

5.2 The matters for QPP 5.1 are the following—

(a) the identity and contact details of the agency;

(b) if—

(i) the agency collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the agency has collected the personal information;

the fact that the agency collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised under an Australian law, or a court or tribunal order—the fact that the collection is required or authorised, including the name of the Australian law, or details for the court or tribunal order, that requires or authorises the collection;

(d) the purposes for which the agency collects the personal information;

(e) the main consequences, if any, for the individual if all or some of the personal information is not collected by the agency;

(f) any other agency or entity, or the kinds of any other agencies or entities, to which the agency usually discloses personal information of the kind collected by the agency;

(g) that the QPP privacy policy of the agency contains information about how the individual may access the personal information about the individual that is held by the agency and seek the correction of the information;

(h) that the QPP privacy policy of the agency contains information about how the individual may complain about a breach of the QPPs, or any QPP code that binds the agency, and how the agency will deal with the complaint;

(i) whether the agency is likely to disclose the personal information to entities outside of Australia;

(j) if the agency is likely to disclose the personal information to entities outside of Australia—the countries in which the recipients are likely to be located if it is practicable to state those countries in the notification or to otherwise make the individual aware of them.

Part 3 Dealing with personal information

6 QPP 6—use or disclosure of personal information

Use or disclosure

6.1 If an agency holds personal information about an individual that was collected for a particular purpose (the ***primary purpose***), the agency must not use or disclose the information for another purpose (the ***secondary purpose***) unless—

(a) the individual has consented to the use or disclosure of the information; or

(b) QPP 6.2 applies in relation to the use or disclosure of the information.

6.2 This QPP applies in relation to the use or disclosure of personal information about an individual if—

(a) the individual would reasonably expect the agency to use or disclose the information for the secondary purpose and the secondary purpose is—

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised under an Australian law or a court or tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the agency; or

Note—

Permitted general situations are stated in schedule 4, part 1.

(d) the agency is a health agency and a permitted health situation exists in relation to the use or disclosure of the information by the agency; or

Note—

Permitted health situations are stated in schedule 4, part 2.

(e) the agency reasonably believes the use or disclosure of the information is reasonably necessary for one or more enforcement-related activities conducted by a law enforcement agency; or

(f) all of the following apply—

(i) ASIO has asked the agency to disclose the personal information;

(ii) an officer or employee of ASIO authorised in writing by the director-general of ASIO for this paragraph has certified in writing that the personal information is required in connection with the performance by ASIO of its functions;

(iii) the disclosure is made to an officer or employee of ASIO authorised in writing by the director-general of ASIO to receive the personal information; or

Editor's note—

QPP 6.2(f) applies in relation to Queensland agencies and does not correspond to an APP.

(g) all of the following apply—

(i) the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest;

(ii) the use or disclosure does not involve the publication of all or any of the personal information in a form that identifies any individual;

(iii) it is not practicable to obtain the express or implied agreement of each individual the subject of the personal information before the use or disclosure;

(iv) if the personal information is disclosed to another entity—the agency is satisfied on reasonable grounds that the relevant entity will not disclose the personal information to another entity.

Editor's notes—

1 QPP 6.2(g) applies in relation to Queensland agencies and does not correspond to an APP.

2 The *Privacy Act 1988* (Cwlth), schedule 1 includes a privacy principle about the disclosure of personal information that is biometric information or biometric templates to an enforcement body in certain circumstances (see APP 6.3).

There is no equivalent QPP for APP 6.3.

6.4 If—

(a) the agency is a health agency; and

(b) schedule 4, part 2, section 3 applied in relation to the collection of the personal information by the agency;

the agency must take reasonable steps to ensure the information is de-identified before the agency discloses it under QPP 6.1 or QPP 6.2.

Written note of use or disclosure

6.5 If an agency uses or discloses personal information in accordance with QPP 6.2(e), the agency must make a written note of the use or disclosure.

Editor's note—

The equivalent APP includes a provision applying to certain private sector entities (see APP 6.6 and APP 6.7).

7 QPP 7—direct marketing

Editor's note—

The *Privacy Act 1988* (Cwlth), schedule 1 includes a privacy principle prohibiting direct marketing by certain private sector entities (see APP 7).

There is no equivalent QPP for APP 7.

Note—

QPP 6 is relevant to the use or disclosure of personal information for the purpose of direct marketing.

8 QPP 8—cross-border disclosure of personal information

Editor's note—

The *Privacy Act 1988* (Cwlth), schedule 1 includes a privacy principle about requirements for cross-border disclosure of personal information (see APP 8).

There is no equivalent QPP for APP 8.

9 QPP 9—adoption, use or disclosure of government related identifiers

Editor's note—

The *Privacy Act 1988* (Cwlth), schedule 1 includes a privacy principle regulating the adoption, use or disclosure of government related identifiers by certain private sector entities (see APP 9).

There is no equivalent QPP for APP 9.

Part 4 Integrity of personal information

10 QPP 10—quality of personal information

10.1 An agency must take reasonable steps to ensure the personal information the agency collects is accurate, up to date and complete.

10.2 An agency must take reasonable steps to ensure the personal information the agency uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

11 QPP 11—security of personal information

11.1 If an agency holds personal information, the agency must take reasonable steps to protect the information—

(a) from misuse, interference or loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If—

(a) an agency holds personal information about an individual; and

(b) the agency no longer needs the information for a purpose for which the information may be used or disclosed by the agency under the QPPs; and

(c) the information is not contained in a public record; and

(d) the agency is not required under an Australian law, or a court or tribunal order, to retain the information;

the agency must take reasonable steps to destroy the information or to ensure the information is de-identified.

Part 5 Access to, and correction of, personal information

12 QPP 12—access to personal information

Access

12.1 If an agency holds personal information about an individual, the agency must, on request by the individual, give the individual access to the information.

Exception to access

12.2 If the agency is required or authorised to refuse to give the individual access to the personal information under—

(a) the Right to Information Act; or

(b) another law in force in Queensland that provides for access by people to documents;

then, despite QPP 12.1, the agency is not required to give access to the extent the agency is required or authorised to refuse to give access.

Editor's notes—

1 The equivalent APP includes a provision applying to certain private sector entities (see APP 12.3).

2 The *Privacy Act 1988* (Cwlth), schedule 1 includes privacy principles about the procedures for requesting access to personal information, including requirements for dealing with requests for access, other means of access, access charges and refusals to give access (see APPs 12.4 to 12.10).

There are no equivalent QPPs for APPs 12.3 to 12.10.

13 QPP 13—correction of personal information

Correction

13.1 If—

(a) an agency holds personal information about an individual; and

(b) either—

(i) the agency is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(ii) the individual requests the agency to correct the information;

the agency must take reasonable steps to correct the information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Editor's note—

The *Privacy Act 1988* (Cwlth), schedule 1 includes privacy principles about requirements to notify other APP entities of corrections to personal information, and refusals to correct personal information (see APPs 13.2 and 13.3).

There are no equivalent QPPs for APPs 13.2 and 13.3.

Request to associate a statement

13.4 If—

(a) the agency refuses to correct the personal information as requested by the individual; and

(b) the individual requests the agency to associate with the information a statement that the information is inaccurate, out of date, incomplete, irrelevant or misleading;

the agency must take reasonable steps to associate the statement in a way that will make the statement apparent to users of the information.

Editor's note—

The *Privacy Act 1988* (Cwlth), schedule 1 includes a privacy principle about dealing with requests to correct personal information (see APP 13.5).

There is no equivalent QPP for APP 13.5.

13.6 An agency need not comply with QPP 13.1 in relation to a request made to the agency to correct personal information if the agency is required or authorised to refuse to correct or amend the information under the Right to Information Act or

another Act regulating the amendment of personal information.

Editor's note—

QPP 13.6 applies in relation to Queensland agencies and does not correspond to an APP.

Schedule 4 Permitted general situations and permitted health situations

schedule 5, definitions *permitted general situation* and *permitted health situation*

Part 1 Permitted general situations

1 Collection, use or disclosure

A permitted general situation exists in relation to the collection, use or disclosure by an agency of personal information about an individual if—

(a) both of the following apply—

(i) it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure;

(ii) the agency reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or safety; or

(b) both of the following apply—

(i) the agency has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the agency's functions or activities has been, is being or may be engaged in;

(ii) the agency reasonably believes that the collection, use or disclosure is necessary in order for the agency to take appropriate action in relation to the matter; or

(c) both of the following apply—

(i) the agency reasonably believes that the collection, use or disclosure is reasonably necessary to assist

an entity to locate a person who has been reported as missing;

(ii) the collection, use or disclosure complies with a guideline in effect under chapter 3, part 2; or

(d) the collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim; or

(e) the collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

Part 2 Permitted health situations

2 Collection—provision of a health service

(1) A permitted health situation exists in relation to the collection by a health agency of health information about an individual if—

(a) the information is necessary to provide a health service to the individual; and

(b) either—

(i) the collection is required or authorised under an Australian law; or

(ii) the individual would reasonably expect the health agency to collect the information for that purpose.

(2) Also, a permitted health situation exists in relation to the collection by a health agency of health information about an individual if—

(a) the information is a family medical history, social medical history or other relevant information about the individual or another individual; and

(b) it is necessary to collect the information about the individual for the purpose of providing the individual or another individual with a health service; and

(c) the information about the individual is collected by the health agency from—

(i) the person who is receiving or about to receive the health service; or

(ii) a responsible person for the individual.

3 Collection—research etc.

(1) A permitted health situation exists in relation to the collection by a health agency of health information about an individual if—

(a) the collection is necessary for any of the following purposes—

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose can not be served by the collection of information that does not identify the individual or from which the individual's identity can not reasonably be ascertained; and

(c) it is impracticable for the health agency to seek the individual's consent to the collection; and

(d) the information is collected—

(i) as required or authorised under an Australian law; or

(ii) by a designated person with the approval of the relevant chief executive; or

(iii) in accordance with guidelines approved by the chief executive of the health department for this subparagraph.

(2) In this section—

designated person see the *Hospital and Health Boards Act 2011*, section 139A.

relevant chief executive, of a health agency, means—

(a) if the health agency is a Hospital and Health Service—the health service chief executive or the chief executive of the health department; or

(b) otherwise—the chief executive of the health department.

4 Use or disclosure—research etc.

A permitted health situation exists in relation to the use or disclosure by a health agency of health information about an individual if—

(a) the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety; and

(b) it is impracticable for the health agency to obtain the individual's consent before the use or disclosure; and

(c) the use or disclosure is conducted in accordance with guidelines approved by the chief executive of the health department for this paragraph; and

(d) for disclosure—the health agency reasonably believes the entity receiving the health information will not disclose the health information or personal information derived from the health information.

5 Disclosure—responsible person for an individual

A permitted health situation exists in relation to the disclosure by a health agency of health information about an individual if—

(a) the health agency provides a health service to the individual; and

(b) the recipient of the information is a responsible person for the individual; and

(c) the individual is—

(i) physically or legally incapable of giving consent to the disclosure; or

(ii) physically can not communicate consent to the disclosure; and

(d) a health professional providing the health service for the organisation is satisfied—

(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(e) the disclosure is not contrary to any wish—

(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the health professional is aware, or of which the health professional could reasonably be expected to be aware; and

(f) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (d).

Schedule 5 Dictionary

section 11

accessible agency website means a website that is—

(a) accessible by members of the public; and

(b) operated by an agency.

access law means a law of the State that provides for access by persons to documents.

affected individual, in relation to a data breach of an agency, see section 47(1)(a)(ii) and (b)(ii).

agency see section 18.

APP means an Australian Privacy Principle set out in the *Privacy Act 1988* (Cwlth), schedule 1.

approved form means a form approved under section 200.

ASIO means the Australian Security Intelligence Organisation established under the *Australian Security Intelligence Organisation Act 1979* (Cwlth).

Assembly means the Legislative Assembly.

Australian law, for schedules 3 and 4, means a law of the Commonwealth or a State, and includes the common law.

authorised officer means a person who holds office under chapter 3A, part 5 as an authorised officer.

bound contracted service provider means the contracted service provider under a service arrangement if—

(a) under section 35(1) and (2), the contracting agency is required to take all reasonable steps to ensure the contracted service provider is required to comply with the privacy principle requirements as if it were the contracting agency; and

(b) under the service arrangement, the contracted service provider is required to comply with the privacy principle requirements as if it were the contracting agency.

collect, for schedules 3 and 4, in relation to personal information, means collect the information for inclusion in a document or generally available publication.

community safety department means the department in which the *Corrective Services Act 2006* is administered.

complainant, for a privacy complaint, means the person who makes the complaint.

compliance notice see section 158.

consent, for schedules 3 and 4, means express consent or implied consent.

contracted service provider see section 34.

contracting agency see section 34.

coroner see the *Coroners Act 2003*.

court includes a justice and a coroner.

data breach, of an agency, means either of the following in relation to information held by the agency—

(a) unauthorised access to, or unauthorised disclosure of, the information;

(b) the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.

de-identify, for schedule 3, in relation to information, means to amend the information so it is no longer about an identified individual, or an individual who is reasonably identifiable from the information.

director-general, of ASIO, means the person appointed as the Director-General of Security under the *Australian Security Intelligence Organisation Act 1979* (Cwlth).

disclose, personal information,, see section 23.

document see section 15.

document to which the privacy principle requirements do not apply see section 16.

eligible data breach, of an agency, see section 47.

enforcement-related activity, for schedule 3, means—

(a) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties or sanctions; or

(b) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(c) the protection of the public revenue; or

(d) the prevention, detection, investigation or remedying of seriously improper conduct; or

(e) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

function includes a power.

generally available publication means a magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public whether or not it is—

(a) published in print, electronically or in any other form; or

(b) available on payment of a fee or charge.

health agency means the health department or a Hospital and Health Service.

health department means the department in which the *Hospital and Health Boards Act 2011* is administered.

health information, about an individual means—

(a) personal information about the individual that includes any of the following—

(i) the individual's health at any time;

(ii) a disability of the individual at any time;

(iii) the individual's expressed wishes about the future provision of health services to the individual;

(iv) a health service that has been provided, or that is to be provided, to the individual; or

(b) personal information about the individual collected for the purpose of providing, or in providing, a health service; or

(c) personal information about the individual collected in connection with the donation, or intended donation, by the individual of any of the individual's body parts, organs or body substances.

health professional see the *Hospital and Health Boards Act 2011*, schedule 2.

health service means—

(a) an activity performed in relation to an individual that is intended or claimed, expressly or otherwise, by the individual or by a person performing the activity—

(i) to assess, record, preserve or improve the individual's health; or

(ii) to diagnose an illness or disability of the individual; or

(iii) to treat an illness or disability of the individual or a suspected illness or disability; or

(b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

health service chief executive see the *Hospital and Health Boards Act 2011*, schedule 2.

held, in relation to personal information, see section 13.

holds, in relation to personal information, see section 13.

Hospital and Health Service means a Hospital and Health Service established under the *Hospital and Health Boards Act 2011*, section 17.

identity card, for a provision about authorised officers, means an identity card issued under section 64.

information commissioner means the information commissioner under the Right to Information Act.

law enforcement agency means—

(a) for the purposes of QPP 6—an enforcement body within the meaning of the *Privacy Act 1988* (Cwlth) or any entity mentioned in paragraph (b); or

(b) otherwise—

(i) the Queensland Police Service under the *Police Service Administration Act 1990*; or

(ii) the Crime and Corruption Commission; or

(iii) the community safety department; or

(iv) any other agency, to the extent it has responsibility for—

(A) the performance of functions or activities directed to the prevention, detection, investigation, prosecution or punishment of offences and other breaches of laws for which penalties or sanctions may be imposed; or

(B) the management of property seized or restrained under a law relating to the confiscation of the proceeds of crime; or

(C) the enforcement of a law, or of an order made under a law, relating to the confiscation of the proceeds of crime; or

(D) the execution or implementation of an order or decision made by a court or tribunal; or

(E) the protection of public revenue.

Minister includes an Assistant Minister.

officer, in relation to an agency, includes—

(a) the agency's principal officer; and

(b) a member of the agency; and

(c) a member of the agency's staff; and

(d) a person employed by or for the agency.

OIC means the office of the information commissioner under the Right to Information Act.

parliamentary committee means—

(a) if the Legislative Assembly resolves that a particular committee of the Assembly is to be the parliamentary committee under this Act—that committee; or

(b) if paragraph (a) does not apply and the standing rules and orders state that the portfolio area of a portfolio committee includes the privacy commissioner—that committee; or

(c) otherwise—the portfolio committee whose portfolio area includes the department, or the part of a department, in which this Act is administered.

permitted general situation means a permitted general situation described in schedule 4, part 1.

permitted health situation means a permitted health situation described in schedule 4, part 2.

personal information see section 12.

portfolio area see the *Parliament of Queensland Act 2001*, schedule.

portfolio committee see the *Parliament of Queensland Act 2001*, schedule.

principal officer means—

(a) in relation to a department—the chief executive of the department; or

(b) in relation to a local government—the chief executive officer (however described) of the government; or

(c) in relation to a government owned corporation—the chief executive officer (however described) of the government owned corporation; or

(d) in relation to a subsidiary of a government owned corporation—the principal officer (however described) of the subsidiary; or

(e) in relation to a public authority for which a regulation declares an office to be the principal office—the holder of the office; or

(f) in relation to another public authority—

(i) if it is an incorporated body that has no members—the person who manages the body's affairs; or

(ii) if it is a body (whether or not incorporated) that is constituted by 1 person—the person; or

(iii) if it is a body (whether or not incorporated) that is constituted by 2 or more persons—the person who is entitled to preside at a meeting of the body at which the person is present.

privacy commissioner means the Privacy Commissioner appointed under this Act.

privacy complaint see section 164.

privacy principle requirements means—

(a) for an agency—the requirements under chapters 2 and 3 applying to the agency; or

(b) for a bound contracted service provider—the requirements under chapter 2, parts 1 and 2 and section 41 applying to the service provider under section 36(1).

publication includes a book, magazine or newspaper.

public authority has the meaning given by section 21.

public library includes—

(a) the State library; and

(b) a local government library; and

(c) a library in the State that forms part of a public tertiary educational institution.

public record means a public record under the *Public Records Act 2023*.

QPP see section 26.

QPP code see section 40(1).

QPP privacy policy, for schedule 3, see QPP 1.3.

relevant entity means an agency or bound contracted service provider.

respondent, for a privacy complaint, see section 164.

response period, for a privacy complaint to a relevant entity, for chapter 5, part 1, see section 164A(1).

responsible person, for an individual, for schedule 4, means—

(a) a parent of the individual; or

(b) a child or sibling of the individual if a health professional believes the child or sibling has capacity; or

(c) a spouse of the individual; or

(d) a relative of the individual if the relative is a member of the individual's household; or

(e) a guardian of the individual; or

(f) a person exercising a power under an enduring power of attorney made by the individual that is exercisable in relation to decisions about the individual's health; or

(g) a person who has sufficient personal interest in the health and welfare of the individual; or

(h) a person nominated by the individual to be contacted in case of emergency.

Right to Information Act means the *Right to Information Act 2009*.

RTI commissioner means the RTI commissioner under the Right to Information Act.

sensitive information, for an individual, means the following—

(a) information or an opinion, that is also personal information, about the individual's—

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual orientation or practices; or

(ix) criminal record;

(b) health information about the individual;

(c) genetic information about the individual that is not otherwise health information;

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.

serious harm, to an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example—

(a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure; or

(b) serious harm to the individual's reputation because of the access or disclosure.

service arrangement see section 34.

solicit, for schedule 3, by an entity in relation to personal information, means ask another entity to provide the personal information, or to provide information of a kind in which the personal information is included.

standing rules and orders see the *Parliament of Queensland Act 2001*, schedule.

subsidiary see the *Government Owned Corporations Act 1993*.

use, personal information, see section 23.