Title: Privacy Policy

Responsible Officer: **Registrar**

Action Officer: **Registrar**

References:
Family Responsibilities Commission:

- Queensland Public Service Code of Conduct
- Information Sharing Protocol
- Right to Information Guidelines
- Employee Complaints Management Policy
- External Complaints Management Policy
- Discipline in the Workplace Policy
- Domestic Violence and the Workplace
- Employee Assistance Policy
- Internet Intranet and Email Usage Policy
- Workplace Policy
- Web Privacy and Security Information

Relevant Legislation

- *Family Responsibilities Commission Act 2008*
- *Public Records Act 2002*
- *Right to Information Act 2009*
- *Information Privacy Act 2009*

- *Acts Interpretation Act 1954*
- *Invasion of Privacy Act 1971*
- *Public Service Act (Qld) 2008*
- *Public Sector Ethics Act 1994 (Qld)*
- *Anti-Discrimination Act 1991 (Qld)*

Unit	Family Responsibilities Commission
Manager	Maxine McLeod, Registrar
Author	Maxine McLeod
Position	Registrar
Contact	(07) 4081 8400
Version	4
Issued	December 2017
Authorising Signature	
Review Date	December 2021

Table of Contents

1.0 Purpose

The Queensland Government requires that personal information held by Queensland Government agencies be responsibly and transparently collected and managed in accordance with 11 Information Privacy Principles. The primary intent of the government's *Information Privacy Act 2009* (IP Act) is to protect the privacy of an individual's personal information in the delivery of government services and the conduct of government business. The purpose of this policy is to assist staff of the Family Responsibilities Commission (the Commission) in understanding the operation of the IP Act and how this legislation impacts on work practices.

2.0 Family Responsibilities Commission Privacy Statement

The Commission respects and protects people's privacy and collects, stores, uses, and discloses personal information responsibly and transparently. Where legislation does not provide direction for the collection, management, use and disclosure of personal information, the Commission will operate in accordance with the 11 Information Privacy Principles (IPPs) set out in the *Information Privacy Act 2009*.

A Privacy Implementation Plan detailing actions the Commission will take to ensure compliance with the *Information Privacy Act 2009* is provided at Appendix A.

3.0 Information Privacy

The Queensland Government developed the IP Act to ensure that personal information held by Queensland Government agencies is collected lawfully and is protected from unauthorised use, access and disclosure. It also recognises that people can gain access to their own personal information to check its accuracy and request changes if necessary.

The 11 Information Privacy Principles, or IPPs, which have been adapted from the Commonwealth *Privacy Act 1988*, govern the way personal information is collected, used, managed and disclosed. The IPPs can be grouped into five categories:

- collection of personal information (IPPs 1 – 3)
- security of personal information (IPP 4)
- access and amendment of personal information (IPPs 5 –7)
- use of personal information (IPPs 8 – 10) and
- disclosure of personal information (IPP 11).

The complete text of the IPPs is set out in Appendix B.

4.0 Personal Information

The IP Act defines ***personal information*** as:

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

The information does not have to be true, nor does it need to be in written form. The information can be spoken or communicated by another means.

Identity plays a key role in determining whether the information is 'personal'. Identity must be either:

- apparent or
- reasonably ascertainable from the specific information.

Apparent identity is not constituted by reference to various different sources of information. It is identity which is apparent from a particular source of information. Examples of apparent identity are:

- a person's name
- a person's clearly identifiable image in a photo
- information which is so particularised that it is identifiable with a particular individual.

Reasonably ascertainable identity is constituted of information which is cross-referenced, or compared with other sources of information to identify an individual. The lengths to which one must go to ascertain the identity is a determining factor, i.e.:

- can the information received identify an individual from a readily available reference
- how many steps are required to identify the individual
- how difficult is the information to obtain.

5.0 The Family Responsibilities Commission Act 2008

The *Family Responsibilities Commission Act 2008* (the Act) is the core legislation that authorises the collection, use and disclosure of personal information by the Commission.

Part 8 of the Act provides for information exchange about community members between the Commission and other entities to assist the Commission to make decisions under the Act and to support cohesive and coordinated service provision to community members.

Under section 93 of the Act, the Commissioner may ask a prescribed entity to provide relevant information about a person.

'Relevant information' is defined in section 91 of the Act. It includes information that would assist the Commission to:

- consider matters to which an agency notice relates
- decide whether a person is a community member within the jurisdiction of the Commission
- decide whether to hold a conference with a person notified to the Commission
- identify appropriate persons to attend a conference
- make appropriate decisions at a conference, including referrals to services and conditional income management and
- help the Registrar to assess the effectiveness of, and to monitor compliance with, conference decisions.

'Prescribed entities', which can be requested to provide personal information to the Commission are defined in section 90 of the Act to include:

- Department of Child Safety, Youth and Women
- Department of Education
- Department of Housing and Public Works
- Queensland Corrective Services
- Department of Justice and Attorney-General / Supreme, District, Magistrates and Childrens Courts
- Queensland Police Service
- principals of non-State schools
- community support service providers (State and Australian Government entities and non-government organisations) to which a person has been referred
- School Attendance Case Managers.

Section 92 of the Act enables the Commissioner to give a prescribed entity personal information about a person to:

- obtain relevant information from the entity or
- enable the Commission and the entity to coordinate support services for the person.

'Personal information' is defined broadly under section 92(4) of the Act to mean:

> *"…information or an opinion, whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."*

This definition is consistent with the definition of personal information in the IP Act and is a broad definition which would capture any information from which a person's identity can be ascertained.

Section 92(2) of the Act permits the sharing of a person's personal information with the Department of Human Services, Centrelink Secretary for the purpose of deciding whether a person is a community member, or to make appropriate decisions under the Act about the person.

Section 92(3) also permits the sharing of a person's personal information with the following entities, for the purpose of evaluating the effectiveness and operations of the Commission:

- The Commissioner for Children and Young People and Child Guardian
- Department of Child Safety, Youth and Women
- Department of Education
- Department of Housing and Public Works
- Queensland Corrective Services
- Department of Justice and Attorney-General / Supreme, District, Magistrates and Childrens Courts
- Department of Human Services.

6.0 Personal Information Collected by the Commission

To support the objectives of welfare reform, the Commission collects and manages personal information about:

- Centrelink clients with addresses registered in the five welfare reform communities of Aurukun, Coen, Doomadgee, Hope Vale and Mossman Gorge
- individuals who are notified to the Commission through an agency notice.

The Commission also holds limited information about Local Commissioners, and all relevant human resource information on employees, including prospective employees.

The Commission enters into contractual arrangements with external bodies for the supply of goods and services. None of the existing contracts contain personal information.

The Commission does not maintain any public registers.

Further detail about Commission records containing personal information is set out in Appendix C.

7.0 Privacy Contact Officer

The Commission has appointed the following person responsible for dealing with matters under the IP Act (otherwise known as the Privacy Contact Officer):

The Client Manager
PO Box 5438
CAIRNS QLD 4870
Ph: (07) 4081 8400

8.0 How Personal Information is Managed by the Commission

The Commission will collect and manage personal information in accordance with the 11 IPPs contained in the IP Act.

In addition, the Commission will comply with the requirements of the *Public Records Act 2002*, which governs the storage, transfer, management and disposal of Commission records. Under the *Public Records Act 2002* we are required to:

- store and dispose of our administrative records in accordance with the timeframes identified in the *General Retention and Disposal Schedule for Administrative Records* from the Queensland State Archives
- store and dispose of our client and core business records only on approval from the State Archivist.

Section 141 of the Act requires the Commission to destroy copies of agency notices relating to persons whom the Commission confirms are not within its jurisdiction. The Commission policy is for such records to be destroyed as soon as practicable.

9.0 Accessing Personal Information Held by the Commission

IPPs 6 and 7 give individuals the right to access and make amendments to personal information held by the Commission. The right to access or correct personal information held by the Commission is limited to rights under the *Right to Information Act 2009* (RTI Act). Requests for access to, or to amend personal information must be made in writing to:

The Privacy Contact Officer (Client Manager)
PO Box 5438
CAIRNS QLD 4870
Ph: (07) 4081 8400

10.0 Right to Information

The RTI Act is the Queensland Government's approach to giving Queenslanders greater access to information.

The Queensland Government has made a commitment to provide access to information held by the government, unless on balance it is contrary to the public interest to do so. The legislation aims to make more information available, provide equal access to information across all sectors of the community, and provide appropriate protection for individual's privacy.

11.0 Privacy Complaints Process

If you believe that the Commission has not dealt with your personal information in accordance with the Act, or the IP Act, you may make a complaint in writing to the Commission. The complaint should be made within 6 months from the date that the breach occurred. Written complaints should be sent to:

The Privacy Contact Officer (Client Manager)
PO Box 5438
CAIRNS QLD 4870
Ph: (07) 4081 8400

You may telephone the Privacy Contact Officer on 4081 8412 if you need assistance in applying for a review, or if you require more information about the complaints process.

Complaints will be acknowledged in writing within 14 days from the date the complaint was received by the Commission. The Commission will make every effort to process each complaint within 30 business days from the date it was received. The Commission will advise the complainant in writing of the outcome of the Commission's investigation of the complaint within 7 working days of the decision being made. All complaints must be addressed by the Commission and a decision advised to the complainant within 45 days of the complaint being received at the latest.

If a complainant does not agree with the Privacy Contact Officer's decision, they may apply in writing to the Commissioner for a review of the decision.

Applications for review should be made within 28 days of the complainant receiving the initial complaint decision. Applications for review should be sent to the Commissioner at:

FRC Commissioner
PO Box 5438
CAIRNS QLD 4870

The review will be completed within 30 business days of receipt of the application for review. The complainant will be notified in writing of the outcome of the review within 7 business days of the review decision being made.

If a complainant is not satisfied with an internal review, they may complain to the Queensland Ombudsman or the Information Commissioner. Further information about the Queensland Ombudsman's role and jurisdiction can be obtained by telephoning 1800 068 908 or at www.ombudsman.qld.gov.au. Further information concerning complaints to the Information Commission can be obtained by telephoning 07 3234 7373 or at www.oic.qld.gov.au.

12.0 Managing Privacy Breaches

A privacy breach occurs when there is a failure to comply with the Information Privacy Principles. Breaches can be a result of technical problems, human error, inadequate policies and training, a misunderstanding of the law, or a deliberate act. Common privacy breaches include when personal information is lost, stolen or mistakenly disclosed (for example, a USB flash drive is lost or an email is sent to unintended recipients).

If any staff member becomes aware of a privacy breach it should be reported to the Privacy Contact Officer as soon as possible. The Privacy Contact Officer will respond to the breach in consultation with the EMT and the ICT Administrator and with the assistance of relevant staff.

There are five key steps in responding to a privacy breach:

1. Contain the breach
2. Investigate the cause of the breach
3. Evaluate the associated risks
4. Consider notifying affected individuals
5. Prevent a repeat

Further information about the steps that will be taken in the event of a privacy breach is set out below. The first four steps should be carried out concurrently where possible and the last step is to mitigate further risks of a breach.

Containing the breach

In the first instance ***take the steps necessary to contain the breach and work to minimise any damage will be taken***. This may involve recovering the personal information, shutting down the system that has allowed the breach, suspending the activity that has caused the breach or making operational adjustments in regard to security access.

Where information needs to be retrieved, the Privacy Contact Officer and EMT will determine what action is necessary to obtain the information and ensure where possible that copies have not been made, or if copies exist, that the copies are also retrieved.

Investigate the cause of the breach

Determine what has led to the breach occurring. ***Escalate the matter internally as needed***. In all instances the Privacy Contact officer will notify the Commissioner, the Registrar, and the ICT Administrator.

If the breach is considered of major significance, consideration will be given to notifying the Office of the Information Commissioner (OIC), DATSIP Director-General, the Public Service Commission or the Crime and Corruption Commission. If the breach involves theft or criminal activity the Queensland Police Service will be notified as a matter of course.

Reporting all breaches to the Privacy Contact Officer will enable the Commission to maintain a central log of breaches that could be used to remedy future breaches and source solutions to information handling practices.

Evaluate the associated risks

The type of personal information that has been breached will be assessed. Government issued identifiers including Medicare numbers, driver's licence numbers,

health information and financial information will pose a significant risk. A combination of personal information may create a risk of identity theft.

Which individuals and how many individuals have been put at risk by the breach will be determined. Is it possible that certain individuals may be at more risk than others due to their personal circumstances.

The cause of the breach will be assessed. Was it a one-off incident or was it caused from systemic vulnerability? Was the breach a targeted attack? What steps were necessary to contain the breach, has information been recovered and was the breach of a nature which provided easy accessibility to information?

The recipient of the information and how the information could be used will be assessed. Importantly what is the risk of further access, use or disclosure including via media or online?

The impact upon the Commission from a media perspective will be assessed.

Notifying affected individuals

The IP Act does not require an agency to notify individuals who have been affected by a privacy breach, however, in the interests of a commitment to transparent governance, and to mitigate the damage for affected individuals, it is recommended that affected individuals are notified. Affected individuals would then be afforded the opportunity to take steps to protect themselves.

There may be occasions where notification may be counter-productive and cause unnecessary anxiety. Factors that will be considered in deciding whether to notify individuals are:

- What is the risk of harm to the individual?
- What steps have already been taken to avoid or mitigate any actual or potential harm?
- What is the ability of the individual to take further steps to protect themselves?
- Is the information of a sensitive nature, or of such a nature to cause humiliation or embarrassment to the individual?
- Are there any legislative obligations that require the Commission to notify affected individuals?

Where notification may not be warranted is, for example, where a device is lost (e.g. a USB stick) with personal information on it but the device is encrypted and inaccessible without the decrypt information.

An example of where notification would be warranted is where records are inadvertently made accessible to the public which hold information such as names, home addresses, phone numbers, birth dates, salary information and bank account details. In such a case notification should be given at the earliest opportunity. Situations where it may be appropriate to delay notification would be where notification would compromise an investigation into the breach, or reveal a software vulnerability.

Where it is considered necessary to notify individuals, they will be notified directly – by telephone, letter, email or in person. Notification could include:

- information about the breach

- description of information disclosed
- information as to what has not been disclosed
- what the Commission is doing to control or mitigate the harm
- what steps the individual can take to protect themselves and what the Commission will do to assist
- Commission contact details for further queries and advice
- advice regarding the right to lodge a privacy complaint and the option to lodge the complaint with the OIC if they are dissatisfied with the Commission's response.

Preventing a repeat

Upon containing the breach, consideration will be given to the short or long term measures that could be taken to prevent any reoccurrence. Actions could include:

- security audit of both physical and technical security controls
- review of policies and procedures
- review of employee training practices
- review of contractual obligations with contracted service providers

A Privacy Breach Report will be prepared to record the breach and the decisions made, and to aid in responding to future breaches should they occur. This report should reflect an evaluation of how the matter was handled and why the decisions were made.

For further information and assistance regarding this Privacy Policy contact:

The Registrar
Family Responsibilities Commission
Level 3, 107 Lake Street, Cairns
Telephone (07) 4081 8400 Fax (07) 4041 0974

Appendix A

Privacy Implementation Plan

Goal	Tasks
Awareness	• Place the Family Responsibilities Commission's Privacy Policy on the Commission website. • Display a privacy statement in public areas and on the Commission website. • Inform Commission staff about privacy obligations and procedures, and the content of the Privacy Policy. • Include the Privacy Policy in the induction manual for new staff. • Maintain a staff register of acknowledgement that the Privacy Policy has been read and understood. • Review and if required update privacy obligations in the Commission's Workplace Policy.
Review and update policies and procedures	• Review and update as required the Family Responsibilities Commission's Privacy Policy and procedures. • Review and update other relevant Commission policies and procedures to ensure they reflect the requirements of the *Information Privacy Act 2009*. • Review procedures for accessing and amending personal information. • Identify privacy-related risks in risk registers.
Identify relevant legislation	• Identify statutory requirements that impact the implementation of the *Information Privacy Act 2009* and update the Privacy Policy as required.
Contracts, licenses, and outsourcing agreements	• Ensure that privacy clauses are included in any new contracts, service level agreements, memoranda of understanding, and outsourcing agreements where arrangements involve the collection, storage, use or disclosure of personal information on behalf of the Commission.
Implement privacy notices	• Review all information collection points and ensure privacy notices are attached.

Appendix B

Information Privacy Principles

1 IPP 1—Collection of personal information (lawful and fair)

(1) An agency must not collect personal information for inclusion in a document or generally available publication unless—

(a) the information is collected for a lawful purpose directly related to a function or activity of the agency; and

(b) the collection of the information is necessary to fulfil the purpose or is directly related to fulfilling the purpose.

(2) An agency must not collect personal information in a way that is unfair or unlawful.

2 IPP 2—Collection of personal information (requested from individual)

(1) This section applies to the collection by an agency of personal information for inclusion in a document or generally available publication.

(2) However, this section applies only if the agency asks the individual the subject of the personal information for either—

(a) the personal information; or

(b) information of a type that would include the personal information.

(3) The agency must take all reasonable steps to ensure that the individual is generally aware of—

(a) the purpose of the collection; and

(b) if the collection of the personal information is authorised or required under a law—

(i) the fact that the collection of the information is authorised or required under a law; and

(ii) the law authorising or requiring the collection; and

(c) if it is the agency's usual practice to disclose personal information of the type collected to any entity (the ***first entity***)—the identity of the first entity; and

(d) if the agency is aware that it is the usual practice of the first entity to pass on information of the type collected to another entity (the ***second entity***)—the identity of the second entity.

(4) The agency must take the reasonable steps required under subsection (3)—

(a) if practicable—before the personal information is collected; or

(b) otherwise—as soon as practicable after the personal information is collected.

(5) However, the agency is not required to act under subsection (3) if—

(a) the personal information is collected in the context of the delivery of an emergency service; and

Example—

personal information collected during a triple 0 emergency call or during the giving of treatment or assistance to a person in need of an emergency service

(b) the agency reasonably believes there would be little practical benefit to the individual in complying with subsection (3) in the circumstances; and

(c) the individual would not reasonably expect to be made aware of the matters mentioned in subsection (3).

3 IPP 3—Collection of personal information (relevance etc.)

(1) This section applies to the collection by an agency of personal information for inclusion in a document or generally available publication.

(2) However, this section applies to personal information only if the agency asks for the personal information from any person.

(3) The agency must take all reasonable steps to ensure that—

(a) the personal information collected is—

(i) relevant to the purpose for which it is collected; and

(ii) complete and up to date; and

(b) the extent to which personal information is collected from the individual the subject of it, and the way personal information is collected, are not an unreasonable intrusion into the personal affairs of the individual.

4 IPP 4—Storage and security of personal information

(1) An agency having control of a document containing personal information must ensure that—

(a) the document is protected against—

(i) loss; and

(ii) unauthorised access, use, modification or disclosure; and

(iii) any other misuse; and

(b) if it is necessary for the document to be given to a person in connection with the provision of a service to the agency, the agency takes all reasonable steps to prevent unauthorised use or disclosure of the personal information by the person.

(2) Protection under subsection (1) must include the security safeguards adequate to provide the level of protection that can reasonably be expected to be provided.

5 IPP 5—Providing information about documents containing personal information

(1) An agency having control of documents containing personal information must take all reasonable steps to ensure that a person can find out—

(a) whether the agency has control of any documents containing personal information; and

(b) the type of personal information contained in the documents; and

(c) the main purposes for which personal information included in the documents is used; and

(d) what an individual should do to obtain access to a document containing personal information about the individual.

(2) An agency is not required to give a person information under subsection (1) if, under an access law, the agency is authorised or required to refuse to give that information to the person.

6 IPP 6—Access to documents containing personal information

(1) An agency having control of a document containing personal information must give an individual the subject of the personal information access to the document if the individual asks for access.

(2) An agency is not required to give an individual access to a document under subsection (1) if—

(a) the agency is authorised or required under an access law to refuse to give the access to the individual; or

(b) the document is expressly excluded from the operation of an access law.

7 IPP 7—Amendment of documents containing personal information

(1) An agency having control of a document containing personal information must take all reasonable steps, including by the making of an appropriate amendment, to ensure the personal information—

(a) is accurate; and

(b) having regard to the purpose for which it was collected or is to be used and to any purpose directly related to fulfilling the purpose, is relevant, complete, up to date and not misleading.

(2) Subsection (1) applies subject to any limitation in a law of the State providing for the amendment of personal information held by the agency.

(3) Subsection (4) applies if—

(a) an agency considers it is not required to amend personal information included in a document under the agency's control in a way asked for by the individual the subject of the personal information; and

(b) no decision or recommendation to the effect that the document should be amended wholly or partly in the way asked for has been made under a law mentioned in subsection (2).

(4) The agency must, if the individual asks, take all reasonable steps to attach to the document any statement provided by the individual of the amendment asked for.

8 IPP 8—Checking of accuracy etc. of personal information before use by agency

Before an agency uses personal information contained in a document under its control, the agency must take all reasonable steps to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, complete and up to date.

9 IPP 9—Use of personal information only for relevant purpose

(1) This section applies if an agency having control of a document containing personal information proposes to use the information for a particular purpose.

(2) The agency must use only the parts of the personal information that are directly relevant to fulfilling the particular purpose.

10 IPP 10—Limits on use of personal information

(1) An agency having control of a document containing personal information that was obtained for a particular purpose must not use the information for another purpose unless—

(a) the individual the subject of the personal information has expressly or impliedly agreed to the use of the information for the other purpose; or

(b) the agency is satisfied on reasonable grounds that use of the information for the other purpose 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

(c) use of the information for the other purpose is authorised or required under a law; or

(d) the agency is satisfied on reasonable grounds that use of the information for the other purpose is necessary for 1 or more of the following by or for a law enforcement agency—

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties or sanctions;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or

(e) the other purpose is directly related to the purpose for which the information was obtained; or

Examples for paragraph (e)—

1 An agency collects personal information for staff administration purposes. A new system of staff administration is introduced into the agency, with much greater functionality. Under this paragraph, it would be appropriate to transfer the personal information into the new system.

2 An agency uses personal information, obtained for the purposes of operating core services, for the purposes of planning and delivering improvements to the core services.

(f) all of the following apply—

(i) the use is necessary for research, or the compilation or analysis of statistics, in the public interest;

(ii) the use does not involve the publication of all or any of the personal information in a form that identifies any particular individual the subject of the personal information;

(iii) it is not practicable to obtain the express or implied agreement of each individual the subject of the personal information before the use.

(2) If the agency uses the personal information under subsection (1)(d), the agency must include with the document a note of the use.

11 IPP 11—Limits on disclosure

(1) An agency having control of a document containing an individual's personal information must not disclose the personal information to an entity (the ***relevant entity***), other than the individual the subject of the personal information, unless—

(a) the individual is reasonably likely to have been aware, or to have been made aware, under IPP 2 or under a policy or other arrangement in operation before the commencement of this schedule, that it is the agency's usual practice to disclose that type of personal information to the relevant entity; or

(b) the individual has expressly or impliedly agreed to the disclosure; 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) the disclosure is authorised or required under a law; or

(e) the agency is satisfied on reasonable grounds that the disclosure of the information is necessary for 1 or more of the following by or for a law enforcement agency—

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties or sanctions;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or

(f) all of the following apply—

(i) the disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest;

(ii) the disclosure does not involve the publication of all or any of the personal information in a form that identifies the individual;

(iii) it is not practicable to obtain the express or implied agreement of the individual before the disclosure;

(iv) the agency is satisfied on reasonable grounds that the relevant entity will not disclose the personal information to another entity.

(2) If the agency discloses the personal information under subsection (1)(e), the agency must include with the document a note of the disclosure.

(3) If the agency discloses personal information under subsection (1), it must take all reasonable steps to ensure that the relevant entity will not use or disclose the information for a purpose other than the purpose for which the information was disclosed to the agency.

(4) The agency may disclose the personal information under subsection (1) if the information may be used for a commercial purpose involving the relevant entity's marketing of anything to the individual only if, without limiting subsection (3), the agency is satisfied on reasonable grounds that—

(a) it is impracticable for the relevant entity to seek the consent of the individual before the personal information is used for the purposes of the marketing; and

(b) the relevant entity will not charge the individual for giving effect to a request from the individual to the entity that the individual not receive any marketing communications; and

(c) the individual has not made a request mentioned in paragraph (b); and

(d) in each marketing communication with the individual, the relevant entity will draw to the individual's attention, or prominently display a notice, that the individual may ask not to receive any further marketing communications; and

(e) each written marketing communication from the relevant entity to the individual, up to and including the communication that involves the use, will

state the relevant entity's business address and telephone number and, if the communication with the individual is made by fax, or other electronic means, a number or address at which the relevant entity can be directly contacted electronically

Appendix C

Records containing personal information

In the performance of its functions, the Family Responsibilities Commission holds records containing personal information to assist the Commission to:

- identify community members who are failing to comply with their welfare obligations relating to school enrolment and attendance, child safety and welfare matters, unlawful activity and compliance with tenancy obligations
- decide who is within the jurisdiction of the Commission
- decide who the Commission should have a conference with
- decide on appropriate conference outcomes
- monitor compliance with Family Responsibilities Agreements, Orders and Case Plans.

The Commission receives the following data extracts from the Australian Government:

- Data is accessed by the Commission on the Unified Government Gateway site which includes personal information disclosures containing address histories and income management information
- Department of Human Services, Centrelink data extracts on clients with addresses registered in the five welfare reform communities.

The Commission maintains records of agency notices, which are given to the Commission in the following circumstances:

- a person's child is absent from school within a welfare reform community three times in a school term, without reasonable excuse
- a person's child is absent from school outside of a welfare reform community three times in a school term, without reasonable excuse and the principal is aware that the parent lives or has at any time since 1 July 2008 lived in a welfare reform community area for a period of at least 3 months
- a person has a child of school age who is not enrolled in school without lawful excuse and the Chief Executive Officer of the Department of Education is aware that the parent, or their child lives, or has at any time since 1 July 2008 lived in a welfare reform community area for a period of at least 3 months
- a person is the subject of a Child Safety and Welfare Notice and the Chief Executive Officer of the Department of Child Safety, Youth and Women is aware that the notice relates to conduct that occurred in a welfare reform community area, or that the person, the subject of the allegation lives or has at any time since 1 July 2008 lived in a welfare reform community area for a period of at least 3 months
- a person is convicted of an offence, or made subject to a protection order in a Court in a welfare reform community, Cooktown or Mossman, or another Queensland Magistrates Court when the Clerk of the Court has been advised that the offender lives, or has at any time since 1 July 2008 lived, in a welfare reform community area for a period of at least 3 months or
- a person breaches his or her tenancy agreement in relation to social housing in a welfare reform community – for example, by using the premises for an illegal purpose, causing a nuisance or failing to remedy rent arrears.

The Commission maintains records of conference proceedings and outcomes, including:

- notices to attend a conference
- records of conferences
- Family Responsibilities Agreements
- Family Responsibilities Orders and
- Family Responsibilities Case Plans.

The Commission maintains records prepared in monitoring a person's compliance with a Family Responsibilities Agreement, Order and Case Plan, such as progress reports from service providers to which Commission clients have been referred under a Case Plan, and case notes relevant to the client.

The Commission also maintains records prepared in relation to community members who seek voluntary referral to the Commission and enter into voluntary agreements or income management arrangements.

Relevant information about individuals who are notified to the Commission and are within the jurisdiction of the Commission is maintained on an electronic client database. The database may include the following personal information:

- client names, alias, date of birth, address history, details of their children, Centrelink payment history and income management information
- school information inclusive of children's names, date of birth, school being attended, details of carer/parent/grandparent/guardian and addresses
- Court information inclusive of details of convictions, plea and sentence, community service orders/probation orders, DV orders and bail conditions
- Child Safety and Welfare Notices inclusive of substantiated and unsubstantiated allegations, investigation details, details of Intervention and Parental Agreements, Case Plans, Child Safety history and individual's details contained within the Child Safety and Welfare Notice
- tenancy notices inclusive of lease details/occupant details, arrears of rent and damage to property
- Queensland Corrective Services information inclusive of record of imprisonment, release, corrective courses completed
- Queensland Corrective Services, Probation and Parole information including further details on community service orders and probation orders
- conference information inclusive of conference dates, times, names of support persons present, outcomes of conference and decision making process
- service provider information inclusive of client attendance at Wellbeing Centres, Parenting Programs, MPower, Student Case Management Framework, Queensland Health programs and Queensland Corrective Services programs; compliance with Conditional Income Management and secondary referrals
- compliance/non-compliance with Case Plans, details of goals and actions to be completed in the Case Plans and details of appeals or amendments sought to Commission orders/agreements.

Physical client files are also maintained for each individual who has been notified to the Commission and who falls within the jurisdiction of the Commission. The physical client files contain information as detailed above, including additional correspondence.

Relevant information about individuals who are notified to the Commission and are not within the jurisdiction of the Commission is maintained on a physical file. These records are destroyed as soon as practicable.

The Commission holds personal information in relation to employees for the purpose of paying wages and entitlements, monitoring performance and staff training. Records held in relation to Commission employees include:

- employee names, addresses, phone numbers, work histories, training undertaken, tax file details, bank account details, emergency contact details, next-of-kin details inclusive of addresses and phone numbers, selection criteria details, professional development plans and various other human resource documents.