



MANAGEMENT POLICY

Privacy

Document number: MGT-014

This document is the property of LinkWater. It must not be copied or reproduced in any way whatsoever without the authority of LinkWater. This document is uncontrolled when printed. An electronic database manages and stores the controlled version.

Approved on 21 July 2010.

CONTENTS

- 1 PURPOSE 3**
- 2 SCOPE 4**
- 3 PERSONAL INFORMATION..... 4**
 - 3.1 PERSONAL INFORMATION COLLECTED BY LINKWATER.....4
 - 3.2 OTHER INFORMATION COLLECTED5
 - 3.3 E-MAIL.....5
 - 3.4 USE OF PERSONAL INFORMATION.....5
 - 3.5 DISCLOSING PERSONAL INFORMATION TO OTHERS6
 - 3.6 COOKIES6
 - 3.7 SECURITY.....6
 - 3.8 UP-TO-DATE.....6
 - 3.9 WHEN PERSONAL INFORMATION IS NO LONGER NEEDED.....7
- 4 ACCESS OR AMENDMENT APPLICATIONS 7**
- 5 CLASSES OF INFORMATION..... 12**
 - 5.1 THE NATURE, PURPOSE AND CLASSES OF PERSONAL INFORMATION HELD BY LINKWATER12
 - 5.2 RETENTION AND DISPOSAL OF RECORDS.....14
 - 5.3 PROCEDURE TO GAIN ACCESS TO PERSONAL INFORMATION14
- APPENDIX A –INFORMATION PRIVACY PRINCIPLES 15**
- APPENDIX B – EMPLOYEE PERSONNEL RECORDS CONTAINING PERSONAL INFORMATION23**
- APPENDIX C – BUSINESS AND SERVICE DELIVERY RECORDS CONTAINING PERSONAL INFORMATION 26**

1 PURPOSE

LinkWater is committed to protecting the privacy of information collected and managed by LinkWater. LinkWater understands and appreciates that persons providing information to LinkWater are concerned about their privacy and the confidentiality and security of any information that may be provided to LinkWater. LinkWater's customer is the SEQ Water Grid Manager (SEQWGM). LinkWater does not have any individual customers or contracts to transport water to persons other than the SEQWGM, however, LinkWater acknowledges that information is provided to LinkWater from a variety of sources and therefore intends to provide appropriate privacy arrangements.

The Queensland Government has established a privacy regime for the Queensland Public Sector based on 11 Information Privacy Principles (IPPs). LinkWater is bound by these privacy principles pursuant to the *Information Privacy Act 2009* (IP Act). This Privacy Policy outlines personal information LinkWater holds, the purposes for which it is held, and how that information is collected, held, used and disclosed.

LinkWater must comply with the IP Act (including the eleven IPPs) which governs how personal information is collected, stored, used and disclosed. The IP Act also allows for people to access their personal information and request amendments to information held by LinkWater. Appendix A provides the detailed IPPs.

The IPPs deal with the following:

- Principle 1: Collection of personal information (lawful and fair);
- Principle 2: Collection of personal information (requested from individual);
- Principle 3: Collection of personal information (relevance etc.);
- Principle 4: Storage and security of personal information;
- Principle 5: Providing information about documents containing personal information;
- Principle 6: Access to documents containing personal information;
- Principle 7: Amendment of documents containing personal information;
- Principle 8: Checking of accuracy, etc of personal information before use by agency;

- Principle 9: Use of personal information only for relevant purpose;
- Principle 10: Limits on use of personal information; and
- Principle 11: Limits on disclosure.

2 SCOPE

This Policy applies to all employees, consultants and contractors carrying out work directly or indirectly for LinkWater.

3 PERSONAL INFORMATION

Personal information is information about individuals. Personal Information is defined in section 11 of the IP Act 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.

3.1 Personal information collected by LinkWater

LinkWater may collect personal information through its interactions with employees (existing and future), consultants, contractors and/or service providers. The personal information LinkWater collects will vary depending on the circumstances but in all cases LinkWater will only collect information about an individual that is relevant to its business relationship with them. For example, an individual's name, contact details, information about LinkWater's interactions with them and other relevant details that will assist in business dealings. In some cases, LinkWater may be required by law to collect personal information, for example, under workplace, health and safety legislation. If LinkWater does not collect this information, LinkWater may not be able to fulfil an individual's request or provide LinkWater's services.

LinkWater may collect personal information individual's provide from LinkWater's website such as resumes and e-mail addresses. LinkWater will only record this information for the purpose for which it was provided and will not disclose it without obtaining the individual's consent to do so.

LinkWater will sometimes be required to collect the personal information of landholders contiguous or nearby to LinkWater's assets to enable LinkWater to adequately carry out its functions.

3.2 Other information collected

If anyone accesses LinkWater's website, then LinkWater's web servers make a record of the visit and log the following information for statistical purposes only:

- IP address that the request comes from;
- date and time of visit to the site;
- pages accessed and documents downloaded;
- previous site visited but only if a link was followed to LinkWater's website; and
- type of browser used.

No attempt is or will be made to identify users or their browsing activities except in the unlikely event of an investigation where a law enforcement agency may exercise a warrant to inspect activity logs.

3.3 E-mail

As LinkWater is a statutory authority of the Queensland Government, e-mail correspondence sent to LinkWater will be treated as a public record and will be retained as required by the *Public Records Act 2002* and other relevant regulations.

Unless specified, your name and address will not be added to a mailing list, nor will LinkWater disclose these details to third parties without your consent, unless required by law. However, e-mail messages may be monitored by authorised IT staff for purposes such as system troubleshooting and maintenance.

3.4 Use of personal information

LinkWater will use personal information to provide construction, operational, maintenance and asset management services. LinkWater will not use the information for any other purpose unless this is disclosed when the personal information is collected. Accordingly, LinkWater staff are only authorised to access personal information contained in records if this access is necessary to facilitate the purpose for which the information was collected unless one of the exceptions listed within IPP 10 apply.

3.5 Disclosing personal information to others

LinkWater may disclose personal information to a third party where consent is given or the disclosure is permitted or required by law. LinkWater may also be required to disclose information to the following parties and in the following circumstances:

- LinkWater Projects;
- to another organisation if LinkWater transfers constructed assets to that organisation;
- external service providers, such as consultants, contractors (including information technology consultants) or suppliers who LinkWater engages in the provision of LinkWater's services, and auditors, taxation and legal advisers. These service providers are only permitted to use the information for the services or function for which they have been engaged;
- law enforcement agencies to assist in the prevention of criminal activities;
- LinkWater's responsible Ministers; and
- regulatory bodies, government agencies and law enforcement bodies, such as the Australian Tax Office.

3.6 Cookies

LinkWater does not store personal information in cookies. Cookies utilised by LinkWater's website are strictly limited to providing the visitor with the ability to customise the site for return visits or to allow the visitor to carry information across different pages. Cookies are not used to track or identify visitors for any other purpose.

3.7 Security

LinkWater takes all reasonable steps to protect personal information from misuse, loss and unauthorised access, modification or disclosure using physical, electronic and procedural safeguards. To keep electronic information secure, LinkWater uses a range of security measures, such as restricting access to users who have a valid username and password.

3.8 Up-to-date

LinkWater will endeavour to make sure that the personal information, which LinkWater holds, is accurate, complete and up to date. If LinkWater is notified

that the information being held is not accurate, complete or up-to-date, steps will be taken to ensure that it is corrected or the changes to the information are noted.

3.9 When personal information is no longer needed

LinkWater will destroy personal information if it is no longer needed for the purpose for which it was collected or if it is no longer required by law to retain it, using secure methods to destroy or de-identify the information. Hard copy documents are properly disposed of and all electronic information is deleted from LinkWater's systems.

4 ACCESS OR AMENDMENT APPLICATIONS

4.1 Applications

Under section 43 of the IP Act, a person who wishes to be given access to a document(s) of LinkWater (which contains the individual's personal information) may apply for access to the document(s). Under section 44 of the IP Act, a person who has had access to a document(s), whether or not under the IP Act, may apply for amendment of any part of the person's information contained in the document that the person claims is inaccurate, incomplete, out of date or misleading.

An access application must:

- be in the approved form and be accompanied by the application fee;
- give sufficient information concerning the document(s) to enable the Privacy Officer to identify the document(s); and
- state the address to which notices under the IP Act may be sent to the applicant.

An amendment application must:

- be in the approved form;
- provide sufficient information for the Privacy Officer to identify the document;
- state the address to which notices under the IP Act may be sent to the applicant; and
- state the information which is inaccurate, incomplete etc, and requires amendments.

Applicants seeking access or amendment must provide with the application or within 10 business days after the making of the application:

- (a) evidence of identity of the applicant (as prescribed by regulation); and
- (b) if an agent is acting for the applicant – evidence of the agent's authorisation and evidence of identity of the agent.

If LinkWater decides that the access or amendment application is outside the scope of the IP Act then LinkWater will give written notice to the applicant of this decision within 10 business days of receiving the application.

If the access or amendment application does not comply with all relevant application requirements then LinkWater will make reasonable efforts to contact the applicant within 15 business days after receipt of the application. LinkWater will give the applicant a reasonable opportunity to consult with a view to making an application in a form complying with all relevant application requirements. If after giving the applicant the above opportunity and LinkWater decides that the application still does not comply with all relevant application requirements then LinkWater will within 10 business days after making the decision, give the applicant written notice of the decision.

If LinkWater determines that the application could have been made under the *Right to Information Act 2009* (RTI) because the application is for access to a document(s) to the extent it does not contain the personal information of the applicant then LinkWater will within 15 business days after the application is received, inform the applicant that the application is not an application that can be made under the IP Act but can be made under the RTI.

4.2 Refusal to deal with applications

Under the IP Act (and subject to compliance with its provisions), LinkWater may refuse to deal with an application under certain circumstances.

For instance, if an access application is expressed to relate to all documents of a stated subject matter and LinkWater determines that all of the documents consist of exempt information as detailed within section 59 and Schedule 3 of the RTI (which is incorporated by reference in the IP Act), then LinkWater may refuse to deal with the application without having to identify any or all of the documents.

Another example is where LinkWater considers the work involved in dealing with an access or amendment application would substantially and unreasonably divert the resources of LinkWater from LinkWater's use in the performance of its functions.

4.3 Timing of Decision

In the first instance, LinkWater is given 25 business days to make a decision (and give written notice of that decision) on whether amendment of the document(s) is permitted or whether access is to be given to document(s) and if access is to be given – whether any charge must be paid before access is given. Further time is available to LinkWater under the IP Act to make its decision if, for example, under:

- section 55 of the IP Act, LinkWater asks the applicant for a further specified period of time and the criteria in that section are fulfilled; or
- section 56 of the IP Act, in respect of access only, an application involves consultation with a relevant third party; or
- section 57 of the IP Act, the application is transferred from another agency.

4.4 Charges

Under section 79 of the IP Act, before an applicant for an access application for a document is given access to that document, the applicant must pay the applicable access charge for the application.

Fees and charges are determined by a regulation made by Parliament.

4.5 Decision

After considering an access application, LinkWater will –

- decide whether access is to be given to the document(s);
- if access is to be given – decide whether any charge must be paid before access is given; and
- give the applicant written notice of its decision.

If LinkWater has not given written notice of its decision within the specified time then LinkWater is deemed to have made a decision refusing access to the document(s).

After considering an amendment application, LinkWater will –

- decide whether amendment of the document(s) is permitted; and
- give the applicant written notice of its decision.

If LinkWater has not given written notice of its decision within the specified time then LinkWater is deemed to have made a decision refusing to amend the document(s).

4.6 Grounds on which access may be refused

Under section 67 of the IP Act, an access application may be refused under certain circumstances declared in the RTI Act (certain provisions being incorporated by reference in section 67).

LinkWater may refuse to give access to a document if the document is non-existent or unlocatable or access is available through alternative means under section 53 of the RTI.

LinkWater may refuse to give access to the extent a document(s) comprises exempt information. Parliament considers that the disclosure of the exempt information, on balance, to be contrary to public interest. Schedule 3 of the RTI lists the information Parliament considers should be exempt. An example of exempt information is listed below:

- certain Cabinet and Executive Council information; or
- information subject to legal professional privilege; or
- information disclosure of which would found an action for breach of confidence; or
- National or State security information.

Linkwater may refuse to give access to the extent the document(s) comprises information the disclosure of which would, on balance, be contrary to the public interest under section 49 of the RTI. In deciding whether disclosure will be contrary to the public interest, LinkWater will:

- identify and disregard any irrelevant factors, including the factors mentioned in schedule 4, part 1 of the RTI;
- identify any factor favouring disclosure, including any factor mentioned in schedule 4, part 2 of the RTI;
- identify any factor favouring nondisclosure, including any factor mentioned in schedule 4, part 3 or 4 of the RTI; and
- balance any relevant factors favouring disclosure against any factors favouring nondisclosure and decide whether, on balance, disclosure of the information would be contrary to the public interest.

Unless, on balance, the disclosure of the information would be contrary to the public interest, LinkWater will allow access to the information subject to the RTI.

4.7 Grounds on which amendment may be refused

Under section 72 of the IP Act, an amendment application may be refused because the agency is not satisfied, for example:

- that the personal information is inaccurate or incomplete etc; or
- that the information sought to be amended is personal information of the applicant.

4.8 Decision maker

Section 50(2) of the IP Act provides the CEO with the power to delegate the power to deal with an application to another officer of LinkWater, in this case the Privacy Officer.

4.9 Notification of the decision

LinkWater will give written notice of its decision to the applicant in accordance with section 68, 73 and 199 of the IP Act.

4.10 Giving Access

If LinkWater decides to grant access then LinkWater will give access in accordance with section 83 of the IP Act which lists out a range of options in terms of access including inspection or providing a copy of the document(s).

In respect of time limits for access, the applicant may access the documents within 40 business days after the date of the decision to give the person access to the document or any additional period allowed by LinkWater.

4.11 Internal Review

If the applicant is unsatisfied with the decision made he/she may apply for an internal review. The internal review application must be made in writing within 20 business days of the date of the written notice of the decision. The internal review must be conducted within 20 business days by a person other than the Privacy Officer who initially handled the matter and someone who is senior to the Privacy Officer.

4.12 External Review

If the applicant is unsatisfied with the internal review, he/she may apply for an external review. The Information Commissioner is responsible for reviewing decisions under the IP Act and conducts external reviews. Applications for external review must be made in writing within 20 business days of the date of the written notice of the internal review decision.

The address to which those applications must be made is as follows:

Office of the Information Commissioner

Address:

Level 4
300 Adelaide Street
Brisbane Qld 4000

Postal Address:

PO Box 10143
Adelaide Street
Brisbane Qld 4000

There is no charge for an internal or external review.

5 CLASSES OF INFORMATION

5.1 The nature, purpose and classes of personal information held by LinkWater

LinkWater holds electronic and paper records containing personal information. In broad terms, these fall into three categories of personal information relating to:

- staff employment;
- business and service delivery; and
- contractual arrangements with external bodies.

5.1.1 Employee records containing personal information

Employee records (both hard or soft formats) are securely kept by Human Resources (HR) including employment letters, personal details forms, tax declarations, licences and certificates. Personal details, leave and salary information is captured securely by the Business Services Group (Payroll). Training schedules/records for all employees are also maintained by HR. This information is retained for the duration of an officer's employment and then dealt with according to the disposal schedule under the *Public Records Act 2002*.

HR staff can access this information as well as individuals accessing their own information.

Appendix B gives a detailed list of employee personnel records containing personal information.

5.1.2 Business and service delivery records containing personal information

As a statutory authority and a key service provider, LinkWater holds a substantial amount of personal information in its records about individuals, obtained in the course of performing daily functions. These records include:

- consultant/contractor/supplier/vendor records;
- corporate records/financial management records;
- executive governance records such as LinkWater's Board and CEO correspondence;
- information in respect of landholders contiguous or nearby to LinkWater's assets to enable LinkWater to adequately carry out its functions;
- right to information records; and
- knowledge system records.

Appendix C contains a detailed description of the business and service delivery records containing personal information.

5.1.3 Contractual arrangements with external bodies

LinkWater maintains contractual arrangements with external bodies for the supply of goods and services. On occasion some agreements can extend over several years.

The type of contracts, licenses and outsourcing arrangements within LinkWater includes:

- contracts to provide general service delivery products related directly to LinkWater's core business, such as operational services;
- contracts to provide uniform, travel and stationery supplies to LinkWater;
- contracts to supply human resource services to LinkWater, such as the electronic payment of wages into bank accounts and staff employment contracts; and
- licenses to access online digital information products, such as CITEC services.

5.2 Retention and disposal of records

The *Public Records Act 2002* governs the preservation and disposal of public records in Queensland. The Queensland State Archivist is responsible for approving Retention and Disposal Schedules proposed by LinkWater.

The Executive Management Team is responsible for ensuring staff are aware of LinkWater's responsibilities for retention, storage and disposal of corporate records.

5.3 Procedure to Gain Access to Personal Information

General questions regarding the personal information collections or applicants for access to information in a collection, or any personal information held by LinkWater should be dealt with in accordance with the procedures outlined in this Policy and may be directed in the first instance to the Privacy Officer.

The Privacy Officer
LinkWater
PO Box 1045
Spring Hill
Brisbane Qld 4004
Australia

APPENDIX A –INFORMATION PRIVACY PRINCIPLES

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.

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).

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.

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.

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.

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.

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.

IPP 8 – Checking for 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.

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.

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.

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 B – EMPLOYEE PERSONNEL RECORDS CONTAINING PERSONAL INFORMATION

The purpose of these records is to maintain employment history, payroll and administrative information relating to all LinkWater’s employees, whether they are permanent, temporary or contract staff members.

Employee personnel records held by various LinkWater business units are common over the organisation, and therefore are grouped together for ease of comprehension. Not all records are housed in a shared storage facility, and therefore separate security arrangements apply, depending on the level of confidentiality required.

1 Personnel and payroll records

Include:

- competency assessment records;
- declaration of pecuniary interest records;
- exit forms;
- leave applications/approvals;
- letters of appointment, contracts, and other conditions of employment;
- medical records;
- payroll and related information including bank details and electronic payslips;
- performance planning and review records;
- personnel history records;
- personnel registers detailing resignations, retirements, and transfers;
- records relating to personal welfare matters;
- timesheets/attendance/overtime records;
- trade, skill and attitude test records;
- training, license and personal development data;

- travel documentation; and
- workforce planning information.

2 Recruitment records

Include:

- Equal Opportunity forms;
- job applications; and
- resumes.

3 Other records

Include:

- clothing/uniform register;
- emergency contact and after-hours registers (e.g. for staff on-call on incident duty roster);
- incident reports;
- organisational charts; and
- WorkCover reports.

Employee personnel records may include: name, address, date of birth, occupation, qualifications, employee identification number, gender, equal employment information, next of kin, leave details, employment history, work reports and details of pay allowances. They may also include: physical/mental health, disabilities, relationship details, racial or ethnic information, disciplinary investigation, criminal convictions, and personal financial information.

Information held in personnel records may be disclosed outside LinkWater, as appropriate, to:

- Australian Taxation Office;
- Child Support Agency;
- other authorised agencies from time to time as appropriate;
- Queensland Superannuation Office;

- third parties such as banks (information is confirmed but not given);
and
- WorkCover.

APPENDIX C – BUSINESS AND SERVICE DELIVERY RECORDS CONTAINING PERSONAL INFORMATION

1 Corporate records/Financial management records

Corporate records include certain reports and plans that take account of the Business requirements arising from the various laws and policies that the State Government applies to LinkWater.

Other records are collected and maintained to process and account for expenditure, revenue and billing. In general terms the records include information such as name and contact details, financial information including debts, bank details and credit cards. Types of records include:

- Annual Report;
- Budget;
- Business Performance Report;
- Chart of Accounts;
- Operational Plan; and
- Strategic Plan.

2 Knowledge and Information System (KIS) records

LinkWater's network carries processes and stores information and data that supports the core business applications of LinkWater. This includes, e-mail, e-mail addresses (individual and group), internet and intranet activity, information storage and networked directories. Many of these have been described in Appendix B.

In addition there is also personal information stored that relates directly to the user's activities on the KIS. This may include network logins, security identifiers, and internet/intranet usage. KIS administrators log and hold this information. Access is restricted to the Knowledge Manager and appropriate KIS administrators.

When users visit LinkWater's internet site, LinkWater's Internet Service Provider makes a record of the visit and logs the following information for statistical purposes only – the user's server address, the user's top level domain name (for example .com, .gov, .au, etc), the date and time of visit to the website, the pages accessed and documents downloaded, the previous site visited, and the type of browser used. No attempt is or will be made to identify users or their external browsing activities except, in the unlikely event

of an investigation, where a law enforcement agency may exercise a warrant to inspect activity logs.

3 Administration records

These types of records are common throughout LinkWater and include registers such as:

- corporate membership;
- emergency action plans and home contact lists;
- travel booking officer information; and
- workplace, health and safety information.

These records are stored in a variety of media such as paper files, TRIM (LinkWater's document management system), SAP, MS Access, Excel and Word on LinkWater's network. Requests for access to administrative records are provided in accordance with individual need and current policy through the appropriate manager.

4 Consultant/contractor/supplier/vendor records

This type of personal information is collected to assist LinkWater with the engagement of consultants, contractors, suppliers and vendors. The content of these records may include name, address, contact details and occupation. Much of this information has been described in Appendix B and is used to ensure that details are correct for the payment and management of vendors, contractors, and suppliers to LinkWater. This information is retained for as long as necessary, and disposed of under the *Public Records Act 2002*.

A request for access to consultant/contractor/supplier/vendor records is provided according to individual need and current policy, through the appropriate manager and may be subject to RTI requirements.

5 Correspondence registers

LinkWater maintains a number of registers and associated records to provide details of individuals and bodies that have correspondence with it. Examples include executive governance records such as LinkWater's Board and CEO correspondence. The content may include name, address, contact details and occupation. These types of registers are maintained across all units of LinkWater.

A request for access to correspondence registers is provided according to individual need and current policy, through the appropriate manager and may be subject to RTI requirements.

6 Landholder's information

LinkWater will sometimes be required to collect the personal information of landholders contiguous or nearby to LinkWater's assets to enable LinkWater to adequately carry out its functions.