



MANAGEMENT POLICY

Privacy

Document number: MGT-015

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 POLICY 3**
- 2 SCOPE..... 4**
- 3 PERSONAL INFORMATION..... 4**
 - 3.1 PERSONAL INFORMATION COLLECTED BY LINKWATER PROJECTS4
 - 3.2 OTHER INFORMATION COLLECTED4
 - 3.3 E-MAIL.....5
 - 3.4 REQUESTS TO ACCESS PERSONAL INFORMATION.....5
 - 3.5 USE OF PERSONAL INFORMATION.....5
 - 3.6 DISCLOSING PERSONAL INFORMATION TO OTHERS6
 - 3.7 COOKIES6
 - 3.8 SECURITY.....6
 - 3.9 UP-TO-DATE.....7
 - 3.10 WHEN PERSONAL INFORMATION IS NO LONGER NEEDED.....7
 - 3.11 ACCESS TO PERSONAL INFORMATION7
- 4 CLASSES OF INFORMATION..... 7**
 - 4.1 THE NATURE, PURPOSE AND CLASSES OF PERSONAL INFORMATION HELD BY LINKWATER PROJECTS..8
 - 4.2 RETENTION AND DISPOSAL OF RECORDS.....9
 - 4.3 PROCEDURE TO GAIN ACCESS TO PERSONAL INFORMATION9
- APPENDIX A – NATIONAL PRIVACY PRINCIPLES 11**
- APPENDIX B – EMPLOYEE PERSONNEL RECORDS 21**
- APPENDIX C – BUSINESS AND SERVICE DELIVERY RECORDS 24**

1 POLICY

LinkWater Projects is committed to protecting the privacy of information collected and managed by LinkWater Projects. LinkWater Projects understands and appreciates that persons providing information to LinkWater Projects are concerned about their privacy and the confidentiality and security of any information that may be provided to LinkWater Projects. LinkWater Projects acknowledges that information is provided to LinkWater Projects from a variety of sources and therefore intends to provide appropriate privacy arrangements.

The Commonwealth Government has established a privacy regime within the *Privacy Act 1988* (Cth) based on 10 National Privacy Principles (NPPs). LinkWater Projects is bound by these privacy principles pursuant to the *Privacy Act 1988* (Cth). This Privacy Policy outlines personal information held by LinkWater Projects, the purposes for which it is held, and how that information is collected, held, used and disclosed.

LinkWater Projects must comply with the ten NPPs which govern how personal information is collected, stored, used and disclosed. The principles also allow for people to access their personal information and request changes or amendments to information held by LinkWater Projects. Appendix A provides the detailed National Privacy Principles.

The NPPs deal with the following:

- Principle 1: Collection;
- Principle 2: Use and Disclosure;
- Principle 3: Data Quality;
- Principle 4: Data Security;
- Principle 5: Openness;
- Principle 6: Access and Correction;
- Principle 7: Identifiers;
- Principle 8: Anonymity;
- Principle 9: Transborder Data Flows; and
- Principle 10: Sensitive Information.

2 SCOPE

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

3 PERSONAL INFORMATION

Personal information is information about individuals. Personal Information is defined in the *Privacy Act 1988* 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 Projects

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

LinkWater Projects may collect personal information individual's provide from LinkWater Projects' website such as resumes and e-mail addresses. LinkWater Projects 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 Projects will sometimes be required to collect the personal information of landholders contiguous or nearby to LinkWater Projects' assets to enable LinkWater Projects to adequately carry out its functions.

3.2 Other information collected

If anyone accesses LinkWater Projects' website, then LinkWater Projects' 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 the LinkWater Projects' 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 Projects is a corporation the shares of which are owned by the Queensland Government, e-mail correspondence sent to LinkWater Projects 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 Projects 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 Requests to access personal information

Requests to update personal information, such as a change of address, should be directed to the LinkWater Projects business unit which currently holds the personal information. The Privacy Contact Officer is the appropriate point of contact if there are issues concerning access to personal information. The Privacy Officer can advise on access to personal information and legislative requirements governing such access.

3.5 Use of personal information

LinkWater Projects will use personal information to provide construction, operational, maintenance and asset management services. LinkWater Projects will not use the information for any other purpose unless this is disclosed when the personal information is collected. Accordingly, LinkWater Projects 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 or the access is permitted or required by law.

3.6 Disclosing personal information to others

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

- LinkWater;
- to another organisation if LinkWater Projects transfers constructed assets to that organisation;
- non-owner participants in LinkWater Projects' alliances for construction;
- external service providers, such as consultants, contractors (including information technology consultants) or suppliers who LinkWater Projects engages in the provision of LinkWater Projects' 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;
- the Minister for Infrastructure and Planning; and
- regulatory bodies, government agencies and law enforcement bodies, such as the Australian Tax Office.

3.7 Cookies

LinkWater Projects does not store personal information in cookies. Cookies utilised by LinkWater Projects' 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.

3.8 Security

LinkWater Projects 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 Projects uses a range of security measures, such as restricting access to users who have a valid username and password.

3.9 Up-to-date

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

3.10 When personal information is no longer needed

LinkWater Projects 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 our systems.

3.11 Access to personal information

In most circumstances, LinkWater Projects will allow an individual to access the personal information held about them. However, there are exceptions to this right, for example, access may be denied where LinkWater Projects decides that making the information available would unreasonably impact on the personal information of another person or LinkWater Projects is legally prevented from disclosing this information.

4 CLASSES OF INFORMATION

LinkWater Projects is committed to ensuring that all personal information holdings are managed with reliability and in accordance with the 10 NPPs. This Privacy Policy outlines the steps that LinkWater Projects will take to meet the obligations under the *Privacy Act 1988* (Cth), which include:

- public availability of this privacy policy; and
- the procedure for gaining access to and amending personal information (s 4.3).

Section 4.1 also incorporates the following information:

- the types of personal information that LinkWater Projects holds; and
- existing contracts and outsourcing arrangements identified to this time.

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

LinkWater Projects 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.

4.1.1 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.

4.1.2 Business and service delivery records containing personal information

As a corporate body and a key service provider, LinkWater Projects 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 Projects' Board and CEO correspondence;
- information of landholders contiguous or nearby to LinkWater Projects' assets to enable LinkWater Projects to adequately carry out its functions; and

- knowledge system records.

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

4.1.3 Contractual arrangements with external bodies

LinkWater Projects 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, licences and outsourcing arrangements within LinkWater Projects include:

- contracts to provide general service delivery products related directly to LinkWater Projects' core business, such as construction services;
- contracts to provide uniform, travel and stationery supplies to LinkWater Projects;
- contracts to supply human resource services to LinkWater Projects, 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.

4.2 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 in respect of public records.

The Executive Management Team is responsible for ensuring that staff are aware of LinkWater Projects' responsibilities for retention, storage and disposal of corporate records. These responsibilities must be complied with in relation to *Privacy Act 1988* and the 10 NPPs.

4.3 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 Projects may be directed in the first instance to the Privacy Contact Officer. Access will be provided in accordance with the *Privacy Act 1988* and the NPPs.

The Privacy Contact Officer
LinkWater Projects
PO Box 1045
Spring Hill
BRISBANE QLD 4004
Australia

APPENDIX A – NATIONAL PRIVACY PRINCIPLES

1 Collection

- 1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.
- 1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.
- 1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:
 - (a) the identity of the organisation and how to contact it; and
 - (b) the fact that he or she is able to gain access to the information; and
 - (c) the purposes for which the information is collected; and
 - (d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
 - (e) any law that requires the particular information to be collected; and
 - (f) the main consequences (if any) for the individual if all or part of the information is not provided.
- 1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.
- 1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2 Use and Disclosure

- 2.1 An organisation must not use or disclose personal information about an individual for a purpose (**the secondary purpose**) other than the primary purpose of collection unless:
 - (a) both of the following apply:
 - (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
 - (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or
 - (b) the individual has consented to the use or disclosure; or

- (c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
 - (i) it is impracticable for the organisation to seek the individual's consent before that particular use; and
 - (ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
 - (iii) the individual has not made a request to the organisation not to receive direct marketing communications; and
 - (iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and
 - (v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or
- (d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:
 - (i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
 - (ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and
 - (iii) in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or
- (e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:
 - (i) a serious and imminent threat to an individual's life, health or safety; or
 - (ii) a serious threat to public health or public safety; or
- (ea) if the information is genetic information and the organisation has obtained the genetic information in the course of providing a health service to the individual:
 - (i) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life,

- health or safety (whether or not the threat is imminent) of an individual who is a genetic relative of the individual to whom the genetic information relates; and
- (ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95AA for the purposes of this subparagraph; and
 - (iii) in the case of disclosure—the recipient of the genetic information is a genetic relative of the individual; or
- (f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
- (g) the use or disclosure is required or authorised by or under law; or
- (h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
- (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
 - (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 or prescribed conduct;
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

- 2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

- 2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.
- 2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:
- (a) the individual:
 - (i) is physically or legally incapable of giving consent to the disclosure; or
 - (ii) physically cannot communicate consent to the disclosure; and
 - (b) a natural person (the **carer**) providing the health service for the organisation is satisfied that either:
 - (i) the disclosure is necessary to provide appropriate care or treatment of the individual; or
 - (ii) the disclosure is made for compassionate reasons; and
 - (c) 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 carer is aware, or of which the carer could reasonably be expected to be aware; and
 - (d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).
- 2.5 For the purposes of subclause 2.4, a person is **responsible** for an individual if the person is:
- (a) a parent of the individual; or
 - (b) a child or sibling of the individual and at least 18 years old; or
 - (c) a spouse or de facto spouse of the individual; or
 - (d) a relative of the individual, at least 18 years old and a member of the individual's household; or
 - (e) a guardian of the individual; or
 - (f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or
 - (g) a person who has an intimate personal relationship with the individual; or
 - (h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

child of an individual includes an adopted child, a step-child and a foster-child, of the individual.

parent of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

3 Data Quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

4 Data Security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

5 Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6 Access and Correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

- (a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or

- (b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or
- (c) providing access would have an unreasonable impact upon the privacy of other individuals; or
- (d) the request for access is frivolous or vexatious; or
- (e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or
- (f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- (g) providing access would be unlawful; or
- (h) denying access is required or authorised by or under law; or
- (i) providing access would be likely to prejudice an investigation of possible unlawful activity; or
- (j) providing access would be likely to prejudice:
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or
 - (iii) the protection of the public revenue; or
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;
 by or on behalf of an enforcement body; or
- (k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

- 6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.
- 6.4 If an organisation charges for providing access to personal information, those charges:
- (a) must not be excessive; and
 - (b) must not apply to lodging a request for access.
- 6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.
- 6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.
- 6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7 Identifiers

- 7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:
- (a) an agency; or
 - (b) an agent of an agency acting in its capacity as agent; or
 - (c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.
- 7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.
- Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).
- 7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:
- (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or
 - (b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or

- (c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsections 100(2) and (3).

7.3 In this clause:

identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an **identifier**.

8 Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9 Transborder Data Flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

- (a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or
- (b) the individual consents to the transfer; or
- (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
- (e) all of the following apply:
 - (i) the transfer is for the benefit of the individual;
 - (ii) it is impracticable to obtain the consent of the individual to that transfer;
 - (iii) if it were practicable to obtain such consent, the individual would be likely to give it; or
- (f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

10 Sensitive Information

- 10.1 An organisation must not collect sensitive information about an individual unless:
- (a) the individual has consented; or
 - (b) the collection is required by law; or
 - (c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:
 - (i) is physically or legally incapable of giving consent to the collection; or
 - (ii) physically cannot communicate consent to the collection; or
 - (d) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:
 - (i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;
 - (ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or
 - (e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.
- 10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:
- (a) the information is necessary to provide a health service to the individual; and
 - (b) the information is collected:
 - (i) as required or authorised by or under law (other than this Act); or
 - (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.
- 10.3 Despite subclause 10.1, an organisation may collect 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 cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and
- (c) it is impracticable for the organisation to seek the individual's consent to the collection; and
- (d) the information is collected:
 - (i) as required by law (other than this Act); or
 - (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or
 - (iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:

non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.

APPENDIX B – EMPLOYEE PERSONNEL RECORDS

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

Employee personnel records held by various LinkWater Projects business units are common over the corporation, 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, including archived service cards;
- personnel registers detailing resignations, retirements, and transfers;
- records relating to personal welfare matters;
- timesheets/attendance/overtime records;
- trade, skill and attitude test records;
- training, licence 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 Projects, 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

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 Projects.

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 Corporate records/Financial management records include:

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

2 Knowledge and Information System (KIS) records

The LinkWater Projects network carries processes and stores information and data that supports the core business applications of LinkWater Projects. 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 the LinkWater Projects internet site, LinkWater Projects' 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 Projects 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 Projects' document management system), SAP, MS Access, Excel and Word on the LinkWater Projects 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 Projects 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 Projects. This information is retained for as long as necessary under LinkWater Projects' legislative obligations and then disposed of.

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

5 Correspondence registers

LinkWater Projects 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 Projects 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 Projects.

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

6 Landholder's information

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