



INDEPENDENT
TRANSPORT
SAFETY AND
RELIABILITY
REGULATOR

Privacy Management Plan



Privacy Management Plan

1. ITSRR's PRIVACY OBLIGATIONS

1.1 Introduction

As a statutory authority representing the Crown¹, ITSRR is required to comply with the provisions of the *Privacy and Personal Information Protection Act 1998* (NSW) ("the PPIP Act") and the *Health Records and Information Privacy Act 2002* (NSW) ("the HRIP Act").

Privacy and Personal Information Act 1998 (NSW)

The PPIP Act creates enforceable privacy rights for individuals in relation to personal information held by New South Wales public sector agencies and certain statutory bodies ("agencies").

The PPIP Act is based on twelve Information Protection Principles ("IPPs"), which cover the collection, storage, use and disclosure of personal information. The PPIP Act requires agencies to establish internal review procedures for handling complaints from individuals relating to the privacy of their personal information.

Health Records and Information Privacy Act 2002 (NSW)

The HRIP Act imposes obligations on the public and private sectors in NSW in relation to the protection of health records and health information.

The HRIP Act establishes fifteen Health Privacy Principles ("HPPs") which cover the handling of health information.

Purpose of this plan

This plan is made in accordance with ITSRR's obligation to prepare a Privacy Management Plan under section 33 of the PPIP Act.

In accordance with section 33 of the PPIP Act, this Privacy Management Plan includes provisions relating to the following:

- the policies and practices of ITSRR which ensure compliance with the PPIP Act and the HRIP Act;
- the dissemination of those policies and practices to persons within ITSRR; and
- ITSRR's internal review process for handling complaints under the PPIP Act and the HRIP Act.

1.2 ITSRR's legal framework

To understand ITSRR's practices relating to the personal information and health information of its employees and members of the public it is necessary to understand the purpose and functions of ITSRR. ITSRR operates under the provisions of the *Transport Administration Act 1988* (NSW) ("*Transport Administration Act*"). Section 42C of the *Transport Administration Act* states the principal objective of ITSRR as follows:

To facilitate the safe operation of transport services in the State.

¹ Section 42B, *Transport Administration Act 1988* (NSW)



Privacy Management Plan

ITSRR also has the following objectives:

- (a) to exhibit independence, rigour and excellence in carrying out its regulatory and investigative functions; and
- (b) to promote safety and reliability as fundamental objectives in the delivery of transport services.

The *Transport Administration Act* imposes a range of other obligations on ITSRR relating to its operations, which may affect its handling of personal information.

1.3 What is personal information?

The PPIP Act applies to all personal information. Health information is not personal information for the purposes of the PPIP Act, and is covered separately by the HRIP Act (which is discussed in more detail below).

Personal information means “information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion”². Personal information includes an individual's fingerprints, retina prints, body samples or genetic characteristics, including, relevantly blood samples from random drug testing³.

In order to fall within the definition of personal information, information does not need to clearly identify a person. It need only provide sufficient information to lead to the identification of a person. ‘Personal information’ is not limited to confidential or sensitive personal details.

While the definition of personal information is very broad, there are a number of exceptions to the definition⁴. Relevant to ITSRR, personal information does not include any of the following:

- (a) information about an individual that is contained in a publicly available publication;
- (b) information about an individual that is contained in a protected disclosure within the meaning of the *Protected Disclosures Act 1994*, or that has been collected in the course of an investigation arising out of a protected disclosure;
- (c) information about an individual arising out of a Royal Commission or Special Commission of Inquiry;
- (d) information about an individual that is contained in a document of a kind referred to in clauses 1 or 2 of Schedule 1 (restricted documents) to the [Freedom of Information Act 1989](#) (for example, Cabinet documents or Executive Council documents); and
- (e) information or an opinion about an individual's suitability for appointment or employment as a public sector official.

Personal information is held by a public sector agency if:

² subsection 4(1) of the PPIP Act

³ subsection 4(2) of the PPIP Act

⁴ subsection 4(3) of the PPIP Act



Privacy Management Plan

- (a) the agency is in possession or control of the information;
- (b) the information is in the possession or control of a person employed or engaged by the agency in the course of such employment or engagement; or
- (c) the information is contained in a State record in respect of which the agency is responsible under the *State Records Act 1998*.

Under the PPIP Act, information is not collected by a public sector agency if the receipt of the information by the agency is unsolicited. However, the IPPs relating to the use, disclosure and general handling of personal information will apply to information held by ITSRR which has not been collected by it.

1.4 What is health information?

Health information means:

- (a) personal information or an opinion about:
 - (i) the physical or mental health or a disability (at any time) of an individual; or
 - (ii) an individual's express wishes about the future provision of health services to him or her, or
 - (iii) a health service provided, or to be provided or
- (b) other personal information collected to provide, or in providing, a health service, or
- (c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs, or body substances, or
- (d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of any sibling, relative or descendant of the individual,

but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of the Act⁵.

1.5 The Information Protection Principles

In its handling of personal information, ITSRR is obliged to comply with the Information Protection Principles ("IPPs"). The IPPs are a set of obligations that cover the collection, storage, use and disclosure of personal information.

The IPPs can be reviewed in the context of an organisation's information life cycle, as set out in the Information Management Framework of the NSW Government *Information Management - Privacy and Personal Information Protection Guideline* (July 2002) at <http://www.oict.nsw.gov.au/content/2.3.20-IM-Privacy.asp>

The twelve IPPs are set out in sections 8-19 of the PPIP Act. The PPIP Act also contains a number of exceptions to the operation of the IPPs. A summary of the

⁵ section 6 of the *HRIP Act*



Privacy Management Plan

IPPs, together with a summary of the exceptions to the principles which are likely to be relevant to ITSRR, is set out at Appendix A.

Many of the IPPs require that 'reasonable' steps be taken, having regard to the circumstances. Factors which will be relevant in determining what is 'reasonable' in the circumstances include (but are not limited to): the sensitivity of the information; the possible uses of the information; the circumstances in which it was obtained; and the financial and practical effects of compliance with the IPPs.

1.6 Health Privacy Principles

The HRIP Act sets out fifteen Health Privacy Principles (HPPs) which apply to health information. The HPPs cover collection, retention and security, accuracy and amendment, use and disclosure, and transfer of health information. They also cover access to health information, the use of identifiers, and trans-border data flows.

The HPPs reflect the obligations and concepts in the PPIP Act, in addition to imposing some new obligations. The concept of reasonableness, discussed above in relation to the PPIP Act, is also employed.

The HPPs are set out in Schedule 1 of the HRIP Act. A summary of the HPPs, is set out at Appendix B.

2 EXEMPTIONS AND OTHER MATTERS AFFECTING THE OPERATION OF THE PPIP ACT AND HRIP ACT

2.1 Current policies and laws relating to information

In addition to the PPIP Act and the HRIP Act, a range of legislation affects the way ITSRR handles information. Some legislation will apply to ITSRR as a whole, whereas other acts may only apply to particular parts of the organisation. In many cases, such legislation will restrict or prohibit the disclosure of certain kinds of information in certain circumstances. Other legislation, for example the *Rail Safety Act 2002* and the *Transport Administration Act*, authorises the collection and disclosure of information in certain circumstances.

A number of policy and practical considerations will affect the way ITSRR deals with personal information and health information. It should be remembered that compliance with, or exemption from, the requirements in the PPIP Act and the HRIP Act will not affect obligations or entitlements arising under other legislation or under general law principles.

A list of statutory provisions that may affect the way ITSRR handles personal information and health information is set out at Appendix C. This list is intended to be indicative only, not exhaustive.

2.2 Exemption under the *Transport Administration Act*

Section 42L of the *Transport Administration Act* gives ITSRR a general authority to disclose information (including personal information and health information) where disclosure is necessary for the safe operation of a transport service. Section 42L provides as follows:

- (1) The ITSRR may, if the ITSRR thinks it necessary for the safe operation of a transport service, disclose information acquired by the ITSRR in the performance of the ITSRR's functions under this or any other Act to any other person.



Privacy Management Plan

- (2) The ITSRR may, if the ITSRR thinks it desirable for the promotion of the safe operation of a transport service, publish any information, including the report of a rail safety inquiry or a transport safety inquiry.
- (3) A publication under subsection (2) must not identify a person by name.
- (4) This section does not apply to the disclosure of the whole or part of a train safety record to the Commonwealth or an authority of the Commonwealth under the *Rail Safety Act 2002*.
- (5) This section does not permit the disclosure of information in contravention of section 65A of the *Rail Safety Act 2002* or section 46E of the *Passenger Transport Act 1990*.
- (6) Sections 72 and 73 of the *Rail Safety Act 2002* do not apply to a disclosure permitted under this section.

The *Transport Administration Act* also empowers ITSRR to require transport authorities to provide it with information, including personal information and health information, where this is necessary for ITSRR's safety responsibilities.

2.3 Exemptions under other legislation generally

Generally, ITSRR is exempt from the requirements of the PPIP Act and HRIP Act if, under other legislation, ITSRR must engage in conduct that would constitute a breach of the Act where this is unavoidably part of its safety regulation responsibilities. To illustrate, there are various provisions under the *Rail Safety Act 2002* which would make it necessary to disclose personal information in, for example, safety reports where the name of an individual was essential to making such a report.

3. TYPES OF INFORMATION COLLECTED, HELD AND DISCLOSED BY ITSRR

Given the diversity of functions that ITSRR performs, the range of personal information and health information collected and held by ITSRR is wide. The main types of personal information and health information held by ITSRR are personnel records, rail safety investigations, rail accident and incident reports, and records of the random drug and alcohol testing of transport officers. While it is emphasised that this is not an exhaustive list, some issues relating to these types of information are set out below.

3.1 Employee information collected and held by ITSRR

ITSRR has a substantial amount of personal information and health information relating to its employees and contractors under service agreements.

Personnel records include the following:

- Medical assessment records
- Attendance and leave records
- Recruitment, promotion and transfer records
- Counselling and discipline records
- Performance management and appraisal records
- Training records
- Occupational health and safety records



Privacy Management Plan

- Workers compensation records.

The collection of this personal information is managed in the usual way through a personnel information management system which includes employment history, payroll and leave information.

Personnel information is collected on a central database of employee and contractor information maintained by ITSRR. It is used for payroll and for general management purposes. Information can only be accessed by employees within the Business Services Division and by managers in the business unit in which an employee works.

The personal information and Learning & Development databases are used for all aspects of managing employees and service contractors, including payroll, taxation, administrative and career-related information. It can therefore assist in determining eligibility for promotion and in disciplinary decision-making in the event of an incident relating to a person's performance of their duties. Employee information is not disclosed for any purpose other than in relation to the management of employees.

Access to employee information held on databases is restricted to authorised individuals on the basis of their user identification. Authorisation is generally given to Employee Relations staff in ITSRR Business Services staff and access governed by protocols regarding usage.

In accordance with the requirements of the PPIP Act and HRIP Act, employees can access their payroll information through the Electronic Self Service (ESS) Kiosk and their learning and development by making a request to Business Services.

Employee records are retained while an employment relationship is current. Files on former employees are removed from the system and archived when an employment relationship is terminated.

As part of its obligations pursuant to the PPIP Act and HRIP Act, ITSRR will:

- make employees aware of their right to see their employment records as part of its privacy compliance and awareness strategy.
- ensure administrative procedures are in place to provide a prompt response to an employee's request for access to their learning and development database.
- provide training to staff that handle personnel records in privacy compliance and awareness, and obtain confidentiality undertakings from those who access the database.

Any employee information that is collected to provide statistical information either for internal or external purposes, for example the NSW Premier's Department's annual Workforce Profile and to the Office of the Director of Equal Opportunity in Public Employment will only be used or disclosed in an aggregated and de-identified form.

Grievances are handled according to ITSRR's Grievance Resolution Policy. The policy is based around informal grievance resolution processes. The outcomes of these grievance investigations are usually referred to the Divisional Manager.

ITSRR also participates in employee programs intended to assist employees with particular needs such as the Employee Assistance Program, which helps employees through periods of personal crisis such as bereavement or a marriage breakdown or for counselling after traumatic incidents. These programs are operated externally.

3.2 Safety audits and investigations



Privacy Management Plan

As part of ITSRR's obligations to maintain safety standards, safety incidents are reported. ITSRR also undertakes extensive safety audits to review practices and respond to safety incidents and thereby comply with its obligations under the *Rail Safety Act 2002*. These audits and investigations are performed with specific statutory authority, and so will generally be exempt from the requirements of the PPIP Act and HRIP Act⁶. Having said that, ITSRR will comply with the principles of the PPIP Act and HRIP Act wherever possible.

Investigation procedures involve causation analysis and may include the taking of statements from relevant operational personnel and obtaining information on other circumstances surrounding the event where Regulatory compliance action may be considered as a result of these enquiries. Reports are used as part of ITSRR's reporting obligations to the Minister and referral of reports to the Independent Transport Safety and Reliability Advisory Board, and for internal purposes to recommend further action if necessary.

(a) Collection

In the course of investigations, all relevant information relating to the incident is taken into account. This process may include taking evidence from supervisors and if necessary other employees, as well as members of the public (eg witnesses to incidents). Information about railway employees who have voluntarily provided information about safety matters under the *Rail Safety Act 2002* s 65A (a "whistle blowing" section) is protected except:

- where the employee consents to the disclosure;
- the Chief Investigator or a court is of the opinion that it is necessary in the public interest that the information be disclosed;
- where the Chief Investigator discloses such information to the Chief Executive or any member of staff of the ITSRR.

(b) Disclosure

Information that is disclosed to ITSRR employees and may then form part of a report provided to the Minister or referred to the Independent Transport Safety and Reliability Advisory Board. Under section 42L of the *Transport Administration Act* reports must not identify a person by name. Limited disclosure is permitted under s 65A of the *Rail Safety Act 2002* as described in paragraph (a) above.

As a general principle names will not be disclosed in safety investigations and use will be made of anonymous references (such as "witness A"). However, it may become necessary to disclose names in some circumstances, such as where there are related court proceedings.

(c) Use

The information is used for the purpose of investigating an incident and determining the appropriate follow-up action. It is also used to track safety incidents on the transport system in order to help guide future policy to minimise these risks. In the case of compliance action, prosecution of individuals may occur under the provisions of the Rail Safety Act.

⁶ For example, see sections 66-67 of the *Rail Safety Act 2002* and section 46A of the *Passenger Transport Act 1990*



Privacy Management Plan

(d) Access

Access to the records of investigations is limited to the staff undertaking investigations, staff supervisors, senior managers, the Independent Transport Safety and Reliability Advisory Board and the Minister. Investigation reports from OTSI are tabled in Parliament and published on the OTSI website.

Access may in addition be provided to other authorities when it is legally necessary to do so, such as when a police investigation ensues.

(e) Security and Retention

ITSRR has a comprehensive Records Management Policy which provides for security and retention of records.

3.3. Accreditation procedures

One of the functions of ITSRR is to perform accreditations of transport service providers⁷. These accreditation processes may require applicants to provide both personal and health information to ITSRR. Generally speaking, ITSRR will be authorised to deal with that information in whatever manner is required in order to perform the accreditation. However, ITSRR will comply with the principles of the PPIP Act and HRIP Act wherever possible.

3.4 Drug and alcohol testing of transport officers

ITSRR performs random drug and alcohol testing of railway employees. As ITSRR has specific statutory authority to perform these tests⁸, it is not required to comply with the IPPs or HPPs. However, ITSRR will comply with the principles of the PPIP Act and HRIP Act wherever possible.

4. ACCESS TO PERSONAL INFORMATION AND HEALTH INFORMATION AND THE INTERNAL REVIEW PROCESS

The PPIP Act and HRIP Act provide for:

- (1) access to personal information and health information of a person held by an agency; and
- (2) an internal review process whereby agencies handle complaints about the way in which they have dealt with personal information. An “aggrieved person” (the applicant) can apply to an agency that he or she believes has breached:
 - an IPP or HPP; or
 - provisions of the PPIP Act or HRIP Act relating to personal information kept in a public register.

This part discusses how ITSRR will manage requests for access to personal information and health information and the internal review process.

4.1 Requests for Access

The IPP relating to access to personal information and HPP7 provide that a public sector agency that holds personal information must, at the request of the individual to

⁷ for example, see section 10 of the *Rail Safety Act 2002*.

⁸ Section 42 of the *Rail Safety Act 2002*



Privacy Management Plan

whom the individual relates and without excessive delay or expense, provide the individual with access to the information⁹.

However, an agency is not required to comply with these obligations if:

- (a) the agency is lawfully authorised or required not to comply with the requirements; or
- (b) non-compliance is otherwise permitted, necessarily implied or reasonably contemplated under an Act or any other law¹⁰.

All requests for access to personal information, whether they are made by members of the public or employees, will be dealt with by ITSRR's Freedom of Information/Privacy officer.

The exception to this procedure will be applications by an employee for access to:

- computer records relating to that employee's personnel record; or
- the employee's "hard copy" personnel file (from which the employee may, under supervision, photocopy documents for their information.)

These requests will be dealt with by ITSRR's Human Resources Liaison officer.

The PPIP Act and HRIP Act do not require that requests for access to personal information and health information be in writing.

Where a request for access to personal information or health information is straightforward (for example, an employee of ITSRR may request access to the medical records held by ITSRR about him or her), ITSRR will not require that a formal request be made in writing.

Where the request is not straightforward, ITSRR will ask the person making the request to put it in writing. In this way, ITSRR will obtain clarity about what information access is sought in relation to, and will have a written record of the request on file.

- No charge will be made for employees seeking access to their employee records including for the purpose of altering information or making a notation to personal information;
- For all other requests, fees may be charged.

The FOI/Privacy officer will determine requests:

- for access to personal information held by ITSRR;
- to alter personal information held by ITSRR; and
- to make notations to personal information held by ITSRR

in accordance with the principles set out in the PPIP Act and HRIP Act.

4.2 Internal review

An employee or anyone else can apply to ITSRR for internal review in relation to how ITSRR has dealt with personal information or health information. Applications for internal review may be made when:

⁹ section 14 of the *PPIP Act*; *Sch 1 of the HRIP Act*

¹⁰ section 25 of the *PPIP Act*; *HPP7, Sch 1 of the HRIP Act*



Privacy Management Plan

- (1) a person is dissatisfied with the outcome of a request for access or amendment to personal information or health information; or
- (2) a person considers that an IPP or HPP has been contravened by ITSRR.

Part V of the PPIP Act set out the requirements for the handling of complaints. Complaints under the HRIP Act are also required to be dealt with under Part V of the PPIP Act.

Part V of the PPIP Act provides that an application for review must:

- (1) be in writing;
- (2) be addressed to the public sector agency concerned;
- (3) specify an address in Australia to which the agency can send notification of the outcome of the review;
- (4) be lodged at an office of the public sector agency within 6 months (or such later date as the agency may allow) from the time the applicant first became aware of the conduct the subject of the application; and
- (5) comply with such other requirements as may be prescribed by the regulations to the Act¹¹.

Applicants for internal review are assisted in making an application by the provision of an application form which ensures that all of the information required to constitute an effective application is provided by the applicant. A copy of the form, which is in the format suggested by the Privacy Commissioner, is at Appendix D.

Internal review will be undertaken by Corporate Counsel, or a person nominated by him or her. That person will be, as far as practicable, a person who:

- (a) was not substantially involved in any matter relating to the conduct the subject of the application;
- (b) is an employee or officer of the agency; and
- (c) is otherwise suitably qualified to deal with the matters raised by the application¹².

If there are circumstances that preclude the conduct being carried out by an employee or officer of ITSRR, ITSRR will request that the Privacy Commissioner undertake the review.

ITSRR will acknowledge receipt of the application for review within 14 days of receipt. All applications for internal review will be notified to the Privacy Commissioner as soon as practicable. ITSRR will keep the Privacy Commissioner informed of the progress and findings of the internal review, as well as any action proposed to be taken by ITSRR in relation to the matters the subject of the review¹³.

In reviewing the conduct the subject of the application, the individual dealing with the application will:

- (a) assist the applicant to provide all relevant information and documentation in support of the complaint;

¹¹ section 53 of the *PPIP Act*

¹² see subsection 53(4) of the *PPIP Act*

¹³ see section 54 of the *PPIP Act*



Privacy Management Plan

- (b) the name, position and contact telephone number of the officer who conducted the review;
- (c) consider any relevant material submitted by the applicant and the Privacy Commissioner;
- (d) interview relevant staff, examine records and obtain any other pertinent information on the circumstances of the alleged contravention;
- (e) determine whether the alleged conduct breaches an IPP or HPP and, if so, what harm or damage it has caused the applicant;
- (f) seek advice from the Office of the Privacy Commissioner, where required;
- (g) prepare a report to Executive Director, Corporate Strategy setting out the steps taken in the review, the conclusions reached and a recommendation for action to resolve the complaint.

Following the review, ITSRR will advise the applicant in writing of:

- (a) the findings of the review and the reasons for those findings;
- (b) any action proposed to be taken; and
- (c) the right of the applicant to have the findings and ITSRR's proposed action reviewed by the Administrative Decisions Tribunal ("ADT").

The review may lead to one or more of the following outcomes:

- (a) ITSRR takes no further action;
- (b) ITSRR makes a formal apology to the applicant;
- (c) ITSRR takes remedial action as appropriate, including payment of compensation if necessary;
- (d) ITSRR implements measures to ensure that the conduct does not occur again.

When the outcome of the review indicates that measures need to be implemented by ITSRR to prevent the conduct recurring, implementing these measures and monitoring their compliance will be the responsibility of the relevant manager of that unit in conjunction with the FOI/Privacy Officer and Corporate Counsel.

4.3 External Review

If an individual is not satisfied with the internal review process, they may make an application to the ADT seeking a review of the decision. The ADT may make orders, including the imposition of fines of up to \$40,000 against an agency.

The PPIP Act provides that if the review is not completed within 60 days from the date on which the application is received the applicant is entitled to make an application to the ADT for review.

Among other things, the ADT may make orders requiring ITSRR to:

- (a) refrain from conduct or action which breaches an IPP or HPP;
- (b) correct information disclosed by ITSRR; or
- (c) take steps to remedy loss or damage.



Privacy Management Plan

The ADT may also make an order requiring ITSRR to pay damages of up to \$40,000 for loss or damage suffered where the applicant has suffered financial loss or psychological or physical harm as a result of the conduct.

5. PRIVACY COMPLIANCE STRATEGIES

5.1 General strategies for compliance with the IPPs and HPPs

(a) Collection

ITSRR staff must identify the *purpose* of collecting personal information whenever it is collected, whether directly from individuals or indirectly. Staff must also ensure that collecting the relevant information is necessary to achieve the purpose identified. The *Transport and Administration Act* defines ITSRR's purposes broadly as facilitating the safe operation of transport services in the State through exhibiting independence, rigour and excellence in carrying out its regulatory and investigative functions and promoting safety and reliability as fundamental objectives in the delivery of transport services.

In most circumstances ITSRR collects information from individuals directly. However, information is sometimes collected from third parties, such as for the purpose of investigative functions eg. accreditation audits, compliance audits or compliance investigations.

In relation to employees, the multi-pronged awareness strategy set out in the next section of this plan is intended to achieve the awareness outcomes required under IPP3 and HPP4.

Compliance with these principles requires that all forms used by ITSRR for the collection of personal information include information relating to ITSRR's handling of those records. All forms will be reviewed to ensure that the notification requirements in IPP3 and HPP4 are complied with. In practical terms, this is one of the most important obligations under the PPIP Act and HRIP Act and it is essential that it be addressed in every business unit that collects personal information or health information whether through forms, over the phone, at a counter, or on the website. Nevertheless, it is important to note that exemptions still apply in several situations, including when information is obtained for investigative purposes.

IPP 4 and HPP2 require agencies to limit the collection of personal information and health information respectively to that which is relevant, not excessive, accurate, up-to-date and complete, and not unreasonably intrusive. ITSRR must continually review information systems and practices to ensure these requirements are satisfied. ITSRR's information collection practices broadly conform to this requirement, including information on employees which is consistent with normal business practices. All ITSRR staff will be notified of programs and policies for monitoring of telephone, email and internet usage. In areas where ITSRR's information collection practices are most intrusive, collection is for specific purposes that are likely to be exempt from the requirements of the IPPs and HPPs because they relate to investigation of transport safety, and so are otherwise authorised or required by law.

(b) Retention and security of personal information

ITSRR's retention policies comply with the *State Records Act 1988* and other legal and audit obligations.



Privacy Management Plan

Staff are encouraged through awareness activities to take responsibility for maintaining security standards for manual records and to adopt practices that improve security, such as not leaving databases open on their desktop.

(c) Information about personal information held by ITSRR, access to personal information held by ITSRR and alteration of personal information

The privacy contact officer will be responsible for responding to requests from individuals about ITSRR's holding of personal information relating to that individual. Internal communications relating to the privacy legislation will note that contact should be made with the Privacy Contact Officer if access to information is sought.

Requests for access will be directed to the Privacy Contact Officer. Requests must be made in writing, and the Privacy Contact Officer should gain some assurance of the identity of the individual, in order to avoid disclosing personal information to someone other than the individual to whom that information relates. No charge should be made for the provision of this information.

The process to be used when making such applications is set out in Part 4 of this Plan.

(d) Use and disclosure

Wherever appropriate, forms used by ITSRR will require consent to specific uses of personal information and health information.

All ITSRR staff will be made aware that personal information and health information should only be used or disclosed for the purpose for which it was collected.

IPPs 10 and 11 and HPPs 10 and 11 allow ITSRR to use and disclose personal information and health information to third parties (including external contractors), for a purpose that is directly related to the purpose for which the information was collected. In situations where ITSRR discloses information to third parties as a normal practice, the individual about whom the information relates will be made aware of this when the information is collected.

It is rare for ITSRR to disclose sensitive categories of personal information, such as ethnic or racial origin, religious or philosophical beliefs, trade union membership or health or sexual activities. However, the need to avoid third party disclosure of sensitive information is highlighted in the ITSRR Code of Conduct and Ethics communications and training materials and employees will be encouraged to refer questions about this for further investigation to the Corporate Counsel.

The Privacy Contact Officer (with the advice of the Corporate Counsel) will monitor the activities of Privacy NSW, and keep up to date with current developments in the application of the PPIP Act and HRIP Act.

All information which is disclosed for research purposes will be de-identified.

5.2 Contractors

ITSRR maintains outsourcing relationships with contractors who handle personal information and health information. Examples of outsourcing relationships include the management of payroll/HR systems, Financial Management, IT Support, Employee Assistance Programs and management of insurance including Workers Compensation

ITSRR will ensure that:



Privacy Management Plan

- (a) all organisations and individuals that handle personal information or health information as part of their provisions of services to ITSRR are aware of ITSRR's obligations under the PPIP Act and the HRIP Act;
- (b) all contractors and employees sign a written statement that they will comply with the provisions of the PPIP Act and HRIP Act (where relevant)
- (c) all contracts with external service providers include clauses requiring compliance with the PPIP Act and HRIP Act;
- (d) where necessary, ITSRR will have a right to audit the contractor's handling of personal information (eg. inspection of records); and
- (e) ITSRR is indemnified by contractors for any loss or liability arising from a breach of the PPIP Act or HRIP Act by a contractor.

5.3 Information systems and information security

The overall management of ITSRR's information systems is managed under contractual arrangements.

ITSRR has around 75 PC's including Laptops which are connected to the internal email system and log-on IDs. Registered users have internet access.

Information is backed up on a daily, weekly and monthly basis.

Access to a person's GroupWise email is generally available after a log-on with specific ID and correct password.

No incidents of security breaches or misuses of someone else's email have been recorded.

6 COMMUNICATION OF POLICIES AND PRACTICES

6.1 Availability of Privacy Management Plan

ITSRR's Privacy Management Plan is available electronically via the ITSRR Intranet website.

Hard copies of the plan are available free of charge by writing to the FOI/Privacy officer at the following address:

FOI/Privacy Officer
Independent Transport Safety and Reliability Regulator
Level 22, 201 Elizabeth Street,
Sydney NSW 2000

6.2 Communication and training

All new ITSRR staff, including contractor staff, whether or not their roles involve responsibilities in handling personal information or health information, will receive training to ensure that they:

- (a) are able to identify personal information and health information;
- (b) are aware of the IPPs and HPPs; and
- (c) are aware of the general obligations contained in the PPIP Act and HRIP Act.

Existing staff identified as having specific responsibilities for handling personal information and/or health information will be provided with specific training about their



Privacy Management Plan

obligations under the PPIP Act and HRIP Act. Training will ensure that all line managers and senior management staff are appropriately trained in identifying personal information and health information, complying with the IPPs and HPPs and the obligations imposed on public sector agencies by the PPIP Act and HRIP Act.

Developing a culture of respecting people's right to the privacy of personal information and health information minimises the general risks of ITSRR breaching the legislation such as through:

- an employee accidentally forwarding e-mail communications containing personal information to an individual who does not have a legitimate reason for obtaining this information;
- issuing forms on which personal information is collected without giving notice to employees about information practices such as how the information will be used;
- lax security standards allowing unauthorised access to personal information, such as through someone leaving their computer unattended with sensitive personal information visible on the screen, or files on an employee being left open and unattended on a desk; and
- careless practices such as the disclosure of inaccurate information concerning a former employee to a potential employer with adverse consequences for the job applicant.

Staff training will be supplemented by an e-mail notification to staff that have a GroupWise address highlighting the importance of ITSRR's privacy obligations, the plan to rollout the privacy management plan strategy, and identify where any queries relating to the PPIP Act or HRIP Act should be directed.

6.6 Review and audit

In order to review the implementation of the Privacy Management Plan and identify areas which pose the greatest risk to ITSRR in terms of non-compliance with the PPIP Act and HRIP Act, a review will be conducted at the end of the 2005-06 financial year, ensuring that necessary documentation is in place and, where necessary, changes have been made in work practices.



Appendix A – summary of Information Protection Principles and relevant exceptions

Collection

1. Personal information should be collected lawfully and only when reasonably necessary for the purposes of the agency.
2. Personal information should be collected directly from the person to whom it relates unless that person has authorised collection from someone else or the person is under the age of 16 and the information has been collected from the person's parent or guardian.

Exceptions to Principle 2:

- law enforcement and investigative agencies where compliance might interfere with law enforcement or investigative functions;
 - any agency which is investigating or otherwise handling a complaint which could be referred to an investigative agency;
 - any agency in connection with proceedings before a court or tribunal.
3. When personal information is collected reasonable steps must be taken to ensure that the person to whom it relates is aware:
 - that the information is being collected;
 - of the purposes of collection;
 - of who will receive the information;
 - of whether supply of the information is voluntary and the consequences of a failure to supply the information;
 - of the person's right to access or change the information; and
 - of the name and address of the agency collecting and holding the information.

Exceptions to Principle 3:

- any agency if collected for law enforcement purposes;
- an investigative agency where compliance might interfere with investigative functions;
- any agency which is investigating or otherwise handling a complaint which could be referred to an investigative agency;
- where an agency is authorised or required not to comply under any Act or law;
- where compliance would prejudice the interests of the individual to whom the information relates;
- where the individual expressly consents.

Storage



Privacy Management Plan

4. When personal information has been collected, the agency must take reasonable steps to ensure that the information is relevant to the purpose for which it was collected, not excessive, accurate, up to date, and complete and does not intrude to an unreasonable extent on the personal affairs of the person to whom it relates.
5. When personal information is held by an agency, it must ensure that the information is:
 - kept no longer than is necessary for the purposes for which it is collected;
 - disposed of securely when no longer needed;
 - protected against loss and unauthorised use or dissemination by reasonable security safeguards; and
 - similarly protected if, of necessity, transferred to a person in connection with the provision of a service to the agency, eg, a contractor or consultant.

Exception to Principle 5:

- investigative agencies
6. When personal information is held by an agency, it must take reasonable steps to enable any person to ascertain:
 - whether the agency holds personal information in relation to the person; and
 - the nature, main purposes of holding and how the person may gain access to the information.

Exception to Principle 6:

- where an agency is authorised or required not to comply under any Act or law
7. When an agency holds information about a person it must, on request of the person, provide the person with access to the information without excessive delay or expense.

Exception to principle 7:

- where an agency is authorised or required not to comply under any Act or law
8. When an agency holds information about a person it must, at the request of the person, make appropriate amendments to ensure the information is accurate, up to date, relevant, complete and not misleading.

Exception to Principle 8:

- where an agency is authorised or required not to comply under any Act or law

Use



Privacy Management Plan

9. An agency must not use personal information held by it without taking reasonable steps to ensure that the information is relevant, accurate, up to date, complete and not misleading.
10. An agency must not use personal information other than for the purpose for which it was collected unless:
 - the person who is the subject of the information consents;
 - the other purpose is directly related to the original purpose; or
 - the use of the information for the other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the person or of another person.

Exception to Principle 10:

- where the use is reasonably necessary for law enforcement purposes or the protection of public revenue;
- an investigative agency where compliance might interfere with investigative functions;
- any agency which is investigating or otherwise handling a complaint which could be referred to an investigative agency;
- where an agency is authorised or required not to comply under any Act or law

Disclosure

11. An agency must not disclose personal information to another body, including another public sector agency, unless:
 - the purpose of the disclosure is directly related to the purpose for which the information was collected;
 - the person concerned is reasonably likely to be aware, or has been made aware, that information of that kind is usually disclosed to the body; or
 - the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the person concerned.

Exceptions to Principle 11:

- where disclosure is made in connection with proceedings for an offence or for law enforcement purposes;
- where disclosure is made to a law enforcement agency to locate a person who has been reported to the Police as missing;
- where disclosure is authorised by a subpoena, search warrant or statutory instrument;
- where disclosure is reasonably necessary for the protection of public revenue;
- where disclosure is reasonably necessary in order to investigate an offence where there are reasonable grounds to believe an offence has been committed;



Privacy Management Plan

- an investigative agency where compliance might interfere with investigative functions;
 - any agency which is investigating or otherwise handling a complaint which could be referred to an investigative agency;
 - where the individual expressly consents;
 - any use which relates to a disclosure to another agency administered by the same Minister for the purpose of informing the Minister about a matter under that administration, or to a disclosure to an agency administered by the Premier for the purpose of informing the Premier.
12. An agency should only disclose personal information relating to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership if disclosure is necessary to prevent or lessen a serious and imminent threat to the person's life or health or that of another person.

Exceptions to Principle 12:

- where disclosure is reasonably necessary in order to investigate an offence where there are reasonable grounds to believe an offence has been committed;
- where an agency is authorised or required not to comply under any Act or law;
- where the individual expressly consents;
- any use which relates to a disclosure to another agency administered by the same Minister for the purpose of informing the Minister about a matter under that administration, or to a disclosure to an agency administered by the Premier for the purpose of informing the Premier.



Appendix B – Summary of Health Privacy Principles

HPP 1 Purposes of collection of health information

Collection must be for a lawful purpose that is directly related to a function or activity of the organisation, and is reasonably necessary for that purpose.

Information must not be collected by unlawful means.

HPP 2 Information must be relevant, not excessive, accurate and not intrusive

Information collected must be relevant to the purpose for which it was collected and not excessive and accurate, up to date and complete.

The collection of the information must not intrude to an unreasonable extent on the personal affairs of the individual to whom it relates.

HPP 3 Collection to be from individual concerned

Organisations must collect directly from the individual unless it is unreasonable or impracticable to do so. Collection must be in accordance with any guidelines issued by the Privacy Commissioner.

HPP 4 Individual to be made aware of certain matters

Organisations must take reasonable steps to inform the individual at or before the time of collection (or, if not practicable, as soon as practicable afterwards) of the following:

- (a) the identity of the organisation and how to contact it;
- (b) the fact that the individual is able to request access to the information;
- (c) the purpose of collection;
- (d) persons to whom the organisation usually discloses information of that kind;
- (e) any law that requires the information to be collected; and
- (f) the main consequences (if any) for the individual if the information is not provided.

Where the information is collected from someone else, the organisation must take reasonable steps to make the individual to whom the information relates aware of the above matters except where this would pose a serious threat to the life or health of the individual or collection is in accordance with guidelines by the Privacy Commissioner.

An organisation is not required to comply with the above requirements in certain circumstances such as where the individual consents to non-compliance, non-compliance is otherwise authorised, compliance would prejudice the interests of the individual, the information is required for law enforcement purposes or compliance might detrimentally affect complaint handling or investigative functions of an investigative agency (this extends to public sector agencies in relation to a matter that could be referred to an investigative agency).



Privacy Management Plan

HPP 5 Retention and security

Organisations must ensure that information is kept no longer than necessary, disposed of securely, and protected against loss, unauthorised access, use, modification or disclosure.

Certain investigative bodies are exempt from this provision as are organisations which are lawfully authorised not to comply.

Division 2 of Part 4 of the HRIP Act provides further obligations for private sector persons with regard to the retention of health information. A private sector person who is a *health service provider* must retain health information:

- for seven years if the individual was an adult at the time of collection, or
- until the individual reaches 25 years if, at the time of collection, the individual was under 18.

When a *health service provider* disposes of health information, a record must be kept of the name of the individual, the period covered by the information and the date the information was deleted. Where a *health service provider* transfers information to another organisation and does not retain a record of that information, the health service provider must keep a record of the name and address of the organisation to which the information was transferred. The record may be kept in electronic form, provided it can be printed on paper.

HPP 6 Information about health information held by organisations

Organisations must take reasonable steps to enable an individual to ascertain whether the organisation holds health information relating to that individual and, if it does, the details of that information, the main purpose for which the information is used and the entitlement to access the information.

HPP 7 Access to health information

Where an individual requests access to information about them, an organisation must, without excessive delay or expense, provide the individual with access to the information.

Sections 26 to 32 of Division 3 of Part 4 of the Act contain further details and requirements regarding access to information held by a private sector person. These provisions include that a request for access must be in writing, state the name and address of the individual, details of the information requested and the form in which the person wishes the information to be provided (s26). An individual may authorise another person to have access to the information.

Section 27 requires a private sector person to respond to a request for access within 45 days of receiving the request. If the request is denied the private sector person must provide a written reason for the refusal. If a fee is charged for access, then the private sector person need not provide the individual with access until 7 days after payment provided notice was provided of the fee and that notice is given within 45 days after receiving the request. A failure to respond to a request in accordance with this provision will be taken to be a refusal of access.

Section 28 provides that access is to be provided by giving a copy of the information, or a reasonable opportunity to inspect and take notes.



Privacy Management Plan

Section 29 provides that a private sector person is not required to provide access to information if:

- providing access would pose a serious threat to the life or health of any person and refusing access is in accordance with guidelines, if any, issued by the Privacy Commissioner (note s30 below); or
- providing access would unreasonably impact upon the privacy of another person and refusing access is in accordance with guidelines, if any, issued by the Privacy Commissioner; or
- the information relates to existing or anticipated legal proceedings between the private sector person and the individual and the information would not be accessible by the process of discovery or is subject to legal professional privilege; or
- providing access would reveal the intentions of the private sector person in relation to negotiations, other than about the provision of a health service, with the individual in such a way as to expose the private sector person unreasonably to disadvantage; or
- providing access would be unlawful; or
- denying access is required or authorised by law; or
- providing access would be likely to prejudice an investigation of possible unlawful activity; or
- providing access would be likely to prejudice a law enforcement function; or
- a law enforcement agency performing a lawful security function asks the private sector person not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia; or
- the request has already been made unsuccessfully and there are no reasonable grounds for making the request again; or
- access to the information has already been provided in accordance with the HRIP Act and the individual is making unreasonable, repeated requests for access to the same information.

Section 30 provides that where access is refused on the basis that access would pose a serious threat to the life or health of the individual, the individual may, within 21 days, request that access be provided to a nominated registered medical practitioner.

The notice refusing access must advise the individual of that they may, within 21 days, nominate a medical practitioner to whom access will be provided. Access must then be provided to the medical practitioner within 21 days of this request.

Section 32 provides that nothing in Division 3 is intended to prevent or discourage providing access. However, a private sector person is not to provide access



Privacy Management Plan

otherwise other than as provided for by Division 3 unless the individual has been informed of the requirements of the Division.

HPP 8 Amendment of health information

Organisations must, when requested by the individual, amend personal information to ensure that the information is relevant, up to date, accurate, and not misleading.

If the organisation is not prepared to amend the information, a note must be made on the individual's file noting the amendment request.

Part 3 of the HRIP Act provides that HPP 8 applies to public sector agencies despite HPP8(4) and s21 of the *State Records Act 1998*.

Division 4 of Part 4 contains additional provisions applicable to private sector persons regarding the details to be included in a request for the amendment of information and any refusal to make the requested amendment. If the information is disclosed to another organisation (including any public sector agency or Minister), particulars of the requested amendment must also be provided.

HPP 9 Accuracy

Organisations must ensure that before health information is used reasonable steps are taken to ensure the information is relevant, accurate, up to date, complete and not misleading.

HPP 10 Limits on use of health information

Organisations must not use personal information for a secondary purpose unless one of the following applies:

- (a) the individual consents to the use;
- (b) the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the information to be used for that purpose;
- (c) the use is reasonably believed by the organisation to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual, another person or the public;
- (d) the use is reasonably necessary for the funding, management, planning or evaluation of health services. If the information identifies the individual, the information is not to be published in a generally available publication;
- (e) the use is reasonably necessary for the training of employees and reasonable steps have been taken to de-identify the information. If the information identifies the individual, the information is not to be published in a generally available publication;
- (f) the use is reasonably necessary for research, compilation or analysis of statistics in the public interest and reasonable steps have been taken to de-identify the information. If the information identifies the individual, the information is not to be published in a generally available publication;



Privacy Management Plan

- (g) the use is by a law enforcement agency for the purpose of finding a missing person;
- (h) the use is a necessary part of an investigation when an organisation has reasonable grounds to suspect that:
 - (i) unlawful activity has been/may be engaged in; or
 - (ii) a person may have engaged in unsatisfactory professional conduct/professional misconduct under a health registration Act; or
 - (iii) an employee of the organisation may have engaged in conduct that may be grounds for disciplinary action;
- (i) the use is necessary for the exercise of law enforcement functions by law enforcement agencies when there exists reasonable grounds to believe an offence has been / may be committed;
- (j) the use is reasonably necessary for the exercise of complaint handling or investigative functions by certain investigative agencies. This extends to any public sector agencies investigating or handling a complaint that could be referred to an investigative agency; or
- (k) the use is prescribed by the Regulations.

Nothing in HPP 10 prevents a public sector agency from disclosing information to another agency administered by the same Minister if it is for the purpose of informing the Minister or to an agency under the administration of the Premier to inform the Premier.

HPP 11 Limits of disclosure of health information

Organisations must not disclose information for a secondary purpose unless one of the same criteria in HPP10 applies.

The only additional circumstance where disclosure is authorised is where:

The disclosure is to provide information to an immediate family member of the individual for compassionate reasons. The disclosure must be limited to the compassionate reasons, the individual is incapable of giving consent, disclosure is not contrary to the expressed wishes of the individual and if the immediate family member is under the age of 18, he/she is sufficiently mature.

Nothing in HPP 11 prevents a public sector agency from disclosing information to another agency administered by the same Minister if it is for the purpose of informing the Minister or to an agency under the administration of the Premier to inform the Premier.

HPP 12 Identifiers

Identifiers must not be assigned to individuals unless it is reasonably necessary for the organisation to carry out its functions efficiently.

A private sector person may only adopt the identifier of a public sector agency if the individual has consented to the use, or the use is required or authorised by law.



Privacy Management Plan

HPP 13 Anonymity

Where lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving health services from organisations.

HPP 14 Trans-border data flows and data flow to Commonwealth agencies

Organisations must not transfer health information to any person or body outside the NSW jurisdiction or to a Commonwealth agency unless:

- the organisation reasonably believes that the recipient is bound by privacy principles similar to that of NSW;
- the individual consents to the transfer;
- 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 a request by the individual;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the individual between the organisation and a third party;
- the transfer is for the benefit of the individual, but it is impracticable to obtain consent and the individual would be likely to give consent if it could be obtained;
- the transfer is believed reasonably necessary to prevent serious harm to the life, health or safety of the individual, another person or the public;
- the organisation has taken reasonable steps to ensure the information will be handled consistent with the HPPs; and
- the transfer is required by law.

HPP 15 Linkage of health records

Organisations must not include health information about an individual in a health records linkage system or disclose an identifier of an individual if the purpose is to include the information in a health records linkage system unless the individual has *consented* to the information being included.

A health records linkage system means:

“a computerised system that is designed to link health records for an individual held by different organisations for the purpose of facilitating access to health records, and includes a system or class of systems prescribed by the regulations as being a health records linkage system, but does not include a system or class of systems prescribed by the regulations as not being a health records linkage system.”

Privacy Management Plan



INDEPENDENT
TRANSPORT
SAFETY AND
RELIABILITY
REGULATOR

Appendix C – Legislation affecting handling of information by ITSRR

Transport Administration Act 1988, section 42L

Rail Safety Act 2002, sections 10; 42; 63; 64; 65A; 66; 67; 68; 69; 71; 72; 73

Passenger Transport Act 1990, section 46A; 46D; 46E;



Appendix D – Internal Review Application Form

Privacy Complaint: Internal Review Application Form

This is an applicationⁱ for review of conduct under: *(please choose one - see www.lawlink.nsw.gov.au/privacynsw for further information on the two Acts)*

- s53 of the Privacy and Personal Information Protection Act 1998 (the PPIP Act)
- s21 of the Health Records Information Privacy Act 2002 (the HRIP Act)

1.	Name of the agency ^l you are complaining about:
2.	Your full name:
3.	Your postal address:
4.	<p>If you are complaining on behalf of someone else, write their full name here:</p> <p>What is your relationship to this other person (eg. parent)?</p> <p>Is the other person capable of making the complaint him or herself?</p> <ul style="list-style-type: none"> <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> I'm not sure
5.	What is the specific conduct ^m you are complaining about?
6.	<p>Please tick which of the following describes your complaint: <i>(You can tick more than one)</i></p> <ul style="list-style-type: none"> <input type="checkbox"/> collection of my personal/health information <input type="checkbox"/> security or storage of my personal/health information <input type="checkbox"/> refusal to let me access or find out about my own personal/health information <input type="checkbox"/> accuracy of my personal/health information <input type="checkbox"/> use of my personal/health information <input type="checkbox"/> disclosure of my personal/health information <input type="checkbox"/> other <input type="checkbox"/> I'm not sure
7.	When did the conduct occur? <i>(Please be as specific as you can)</i>



Privacy Management Plan

8.	When did you first become aware of this conduct?
9.	You need to lodge this application within 6 months of the date you have written at Q.8. If more than 6 months has passed, you need to ask the agency for special permission to lodge a late application. If you need to, write here to explain why you have taken more than 6 months to make your complaint:
10.	What effect did the conduct have on you?
11.	What effect might the conduct have on you in the future?
12.	What would you like to see the agency do about the conduct? <i>(For example: an apology, a change in policies or practices, your expenses paid, damages paid to you, training for staff, etc.)</i>
13.	I understand that this form will be used by ITSRR to process my request for an Internal Review. I understand that details of my application will be referred to the Privacy Commissioner in accordance with: section 54 (1) of the Privacy and Personal Information Protection Act 1998; or section 21 of the Health Records and Information Privacy Act 2002; and that the Privacy Commissioner will be kept advised of the progress of the review.
14.	I would prefer the Privacy Commissioner to have: <input type="checkbox"/> a copy of this application form, or <input type="checkbox"/> just the information provided at Q's 5 - 12.

Your signature:

Dated:

NOW SEND THIS FORM TO ITSRR

Keep a copy for your own records too.

ⁱ It is not a requirement under the PPIP Act/the HRIP Act that you complete an application form. This form is designed for your convenience only.

ⁱⁱ The PPIP Act regulates NSW State government departments, Area Health Services, most other State government bodies, and NSW local councils. Each of these is defined as a "public sector agency".

The HRIP Act regulates private and public sector agencies and private sector persons.

ⁱⁱⁱ 'Conduct' can include an action, a decision, or even inaction by the agency. For example the 'conduct' in your case might be a *decision* to refuse you access to your personal information, or the *action* of disclosing your personal information to another person, or the *inaction* of a failure to protect your personal information from being inappropriately accessed by someone else.