Information Privacy Plan

Department of Transport and Main Roads

September 2019

Queensland Government

Creative Commons information

The Queensland Government is committed to providing accessible services to Queenslanders of all cultural and linguistic backgrounds. If you have difficulty understanding this publication and need a translator, please call the Translating and Interpreting Service (TIS National) on 13 14 50 and ask them to telephone the Queensland Department of Transport and Main Roads on 13 74 68.

Document control options

Departmental approvals

Refer to the appropriate Risk Assessment Tool for relevant reviewer and approver.

Date	Name	Position	Action required *(Review/endorse/approve)*	Due
25/09/2019	Graeme Healey	Director, RTI, Privacy and Complaints Management	Reviewed	25/09/2019
25/09/2019	Catherine O'Keeffe	A/General Manager Governance	Endorsed	25/09/2019
26/09/2019	Tracy O'Bryan	Deputy Director General (Corporate)	Endorsed	26/09/2019
28/09/2019	Neil Scales	Director-General	Approved	28/09/2019

Prepared by	Rachel Dando
Title	Principal Advisor (Information Privacy)
Branch & Division	Governance Branch, Corporate Division
Status	Final
DMS ref. no.	

Contents

Introduction

The Department of Transport and Main Roads (the department) is committed to protecting the privacy of individuals through the robust protection of the personal information which it holds. The department collects, stores, uses and discloses personal information responsibly and transparently to deliver services and conduct business.

Objectives

The objective of the Information Privacy Plan is to outline how the department complies with its obligations under the Queensland *Information Privacy Act 2009* (IP Act).

This plan aims to:

- demonstrate to members of the public how the department meets its obligations under the IP Act;
- provide a guideline for employees and contractors of the department who deal with personal information in relation to the functions and activities of the department; and
- illustrate the department's commitment to respecting the privacy rights of staff and members of the public.

Background and Context

In 2009 the Queensland Government introduced the IP Act, establishing a framework for the management of personal information in the Queensland public sector.

Under the IP Act, personal information held by, or under the control of Queensland Government agencies must be collected, stored, used and disclosed in accordance with the 11 Information Privacy Principles (IPPs). The IP Act also provides a complaint mechanism if individuals believe that their personal information has not been dealt with appropriately.

In delivery of its core business, the department holds the most comprehensive collection of personal information of Queenslanders in the Queensland public sector. The department's functions are diverse and extensive, and it is responsible for providing a large range of services, including:

- testing and issuing of driver licences
- inspecting and registering motor vehicles
- improving road safety
- preserving the condition and value of the community's road infrastructure
- upgrading the road network
- maintaining efficient traffic flows
- personalised transport industry
- mass passenger transit including bus, train and ferry
- marine safety, regulating the safety of recreational vessels.

These functions are derived from a range of legislation including the following Acts, and related Regulations:

- *Photo Identification Card Act 2008*
- *Air Navigation Act 1937*
- *Century Zinc Project Act 1997* (ss 5(2)-(7), 11, 12, 13, 21)
- *Civil Aviation (Carriers' Liability) Act 1964*
- *Gold Coast Waterways Authority Act 2012*
- *Heavy Vehicle National Law Act 2012*
- *Maritime Safety Queensland Act 2002*
- *Queensland Rail Transit Authority Act 2013*
- *Rail Safety National Law (Queensland) Act 2017*
- *State Transport Act 1938*
- *State Transport (People Movers) Act 1989*
- *Thiess Peabody Mitsui Coal Pty. Ltd. Agreements Act 1965* (administered by the Minister for Transport and the Commonwealth Games except to the extent administered by the Treasurer, Minister for Aboriginal and Torres Strait Islander Partnerships and Minister for Sport, and the Minister for State Development and Minister for Natural Resources and Mines)
- *Tow Truck Act 1973*
- *Transport Infrastructure Act 1994* (jointly administered by the Minister for Transport and the Commonwealth Games and the Minister for Main Roads, Road Safety and Ports and Minister for Energy, Biofuels and Water Supply)
- *Transport Operations (Marine Pollution) Act 1995*
- *Transport Operations (Marine Safety) Act 1994*
- *Transport Operations (Marine Safety – Domestic Commercial Vessel National Law Application) Act 2016*
- *Transport Operations (Passenger Transport) Act 1994*
- *Transport Operations (Road Use Management) Act 1995*
- *Transport Planning and Coordination Act 1994*
- *Transport (South Bank Corporation Area Land) Act 1999*
- *Transport Security (Counter-Terrorism) Act 2008.*

Personal Information

What is personal information?

Personal information is defined in the IP Act as:

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

Personal information is any information that may lead to the identity of a person. For information to be personal information, two criteria must be satisfied:

- it must be about a living individual, and
- the individual's identity must be apparent or reasonably ascertainable from the information.

There are some obvious examples of personal information such as a person's name and address, but it can also include information about a person's health, criminal or financial records and email addresses.

Information does not have to be true in order to be personal information and it does not need to be written down or recorded in another material form, such as a photograph or audio recording. It can be spoken or communicated in another way, for example, by sign language.

What is not personal information?

Information about a person whose identity is not known or who cannot be readily identified is not covered by the IP Act.

Information about a deceased person, whilst private in nature, is also not considered personal information for the purpose of the IP Act. However, employees are expected to respect the family members of the deceased when using or disclosing such information.

Whilst the IP Act does not apply to company information, it does apply to personal information about an employee of that company.

What is routine personal work information?

Routine personal work information relates solely to the work duties of a public-sector employee and is found in almost all documents held by agencies and Ministers.

When disclosing routine personal work information for a legitimate function of the department, the infringement of a public-sector employee's right to privacy would, generally, be minimal or non-existent as the disclosure would be a matter of expectation in the legitimate course of their employment.

Routine personal work information includes:

- a work email address or work phone number
- authorship of a work document, for example, where the person's name is listed as one of the authors of a report
- a professional opinion given wholly in a professional capacity, for example, a report from a Transport Inspector or a Maritime Safety Officer
- a position classification, for example, "AO6 planning officer"

- a work responsibility, for example, that the officer is the contact person in response to a complaint or query from a member of the public; information about qualifications held where they are required for the officer's position, for example, where a Senior Engineer holds an engineering degree.

Types of personal information collected and held by the department

The department conducts a diverse range of business activities with many functions crucial to the provision of transport services. The collection of personal information is a central part of many of these activities. Personal information held by the department includes, but is not limited to:

- Customer name – including previous names
- Customer address – including address history
- Date of birth
- Digital photographs
- Marital status
- Licence expiry date
- Customer restrictions
- Demerit points
- Driver licence status and history - including details of interstate or international licences, suspensions, cancellations and disqualifications
- Driving and fare evasion offence information
- Information relating to disability parking permits
- Go Card travel information
- Financial information.

Sensitive Information

The department collects personal information that may be considered ‘sensitive’ such as health information, ethnic origin and criminal record. The IPPs within the Qld IP Act do not specifically refer to sensitive information and the department is required to handle all information, including sensitive information, in accordance with the IPPs.

Personnel Records

The department also has obligations in respect of maintaining personal records of its employees. These records are used to maintain all employment activity including payroll, recruitment and associated administrative activity.

Contents of personnel records include personal identifiers and information volunteered or collected as part of a person’s employment history and information required for the department’s business continuity plan such as after-hours emergency contact numbers. Personnel records are kept for variable periods according to the applicable provisions of the general retention and disposal schedule, which is issued by the Queensland State Archives.

How the department manages personal information

The department manages the personal information it holds in accordance with the IPPs contained within the Qld IP Act.

There are 11 IPPs in the IP Act. The IPPs cover the following:

- Collection of personal information (IPPs 1, 2, 3)
- Security of personal information (IPP 4)
- Information about personal information holdings (IPP 5)
- Access and amendment of personal information (IPPs 6, 7)
- Use of personal information (IPPs 8, 9, 10)
- Disclosure of personal information (IPP 11)

The full text of the IPPs is available in schedule 3 of the IP Act.

Collection of personal information

IPPs 1-3 of the IP Act apply where the department requests personal information from a person. Giving notice to individuals about why their personal information is being collected, any authorities under which it is collected and to whom the information is usually disclosed, including anyone they will disclose it to, is essential in promoting transparency about the department's management of personal information.

The department's business units decide what level of information is appropriate to be collected on a case by case basis with the understanding that the details collected must contain enough information as necessary for the particular purpose. The department includes appropriate privacy statements on all forms that collect personal information and provides information to individuals who make contact via our call centre.

Storage and security of personal information

IPP 4 of the IP Act applies to storage and security of personal information. Personal information must be stored securely to prevent loss or misuse. The department takes a proactive and preventative approach to ensure that personal information is held securely, and access is only available to employees to enable them to conduct the required tasks of their role.

Precautions are also taken for the storage of documents that contain protected, confidential and sensitive information. Actions regarding the use of Information and Communication Technology (ICT) facilities and devices are monitored, audited, recorded and reviewed for compliance with departmental policies, standards and the *Code of Conduct for the Queensland Public Service*.

The department is required by legislation to keep and maintain proper records of its activities. To ensure recordkeeping compliance the department is committed to meeting its responsibilities under the *Financial Performance Management Standard 2009*, *Public Records Act 2002* and the Queensland Government Information Standards. All records are kept according to the department's Records Retention and Disposal Schedule, approved by Queensland State Archives.

Access and amendment to personal information

The IP Act provides for a right of access to, and amendment of, personal information in the government's possession or under its control, unless, on balance, it is contrary to the public interest to give the access or allow the information to be amended. Chapter 3 of the IP Act provides a formal mechanism under which an individual can apply to access their personal information. However, where there is an administrative release process available to manage routine requests for information, such as licence and registration information, an individual may seek access under IPP 6 of the IP Act outside the formal process set out in chapter 3.

In general, informal access requests may be made via the online services section of the department's website www.tmr.qld.gov.au, through the department's call centre 13 23 80 or by attending the department's customer service centre. Employees of the department who wish to access their personnel information are to contact their local Human Resource Advisor as the first point of contact.

If the information is not able to be released under an administrative release process, a formal access application can be made via an online application form which is located on the Right to Information (RTI) website, http://www.rti.qld.gov.au. The department may decide to refuse access to certain types of information, either because Parliament has decided that it is exempt information or because releasing it would be contrary to the public interest. Prior to lodging an access or amendment application, the RTI, Privacy and Complaints Management Unit can be contacted on (07) 3306 7108 to discuss any request.

IPP7 relates to the amendment of personal information and requires the department to take all reasonable steps to ensure the accuracy of personal information prior to using it. Similar to accessing personal information, chapter 3 of the IP Act provides a formal mechanism under which an individual can apply to amend their personal information, with IPP 7 providing an informal means of applying for an amendment through a relevant administrative process.

If the department is satisfied that personal information in a document is out of date, inaccurate, incomplete or misleading, it may amend the document either by altering the information or adding a notation to the personal information.

Use and disclosure of personal information

Personal information is valuable, and its loss, inappropriate use or unintended disclosure can have significant consequences for the individual.

IPP 8 and 9 require an agency to ensure the accuracy of personal information before using it, and to only use the parts of personal information that are directly relevant to fulfilling the particular purpose.

IPP10 limits how an agency may use the personal information it holds for another purpose, such as with the individual's consent or for health and safety or law enforcement reasons.

In most circumstances, the department will only use personal information for the purpose it was collected.. The disclosure principle IPP11 sets out when an agency may disclose personal information to someone else, for example another agency. This can only be done in special circumstances, such as with the individual's consent, where a legal authority exists or for some health and safety or law enforcement reasons.

Law Enforcement activity

The term “law enforcement” is defined in the IP Act and contains a number of provisions dealing specifically with the law enforcement activities of law enforcement agencies. These provisions recognise that an agency's use of personal information for investigation and enforcement purposes may not always be compatible with the IPPs in all circumstances. For example, it would defeat the purpose of covert surveillance if an agency were to inform an individual that their personal information is being collected under the collection requirements of IPP2.
Law enforcement activities are dealt with in three different ways in the IP Act:

- as part of the IPPs—the agency is bound by the principles but is able to rely on specific exemptions for law enforcement activities;
- permitted non-compliance with some of the IPPs—the agency can effectively disregard the specified IPPs in relation to an enforcement action;
- exemptions from the IPPs for certain documents—the IPPs do not apply to personal information in the stated documents.

Under the use and disclosure principles of the IP Act, personal information may be used or disclosed to a third party by the department, if the use or disclosure is necessary in relation to one or more of the following activities:

- prevention, detection, investigation, prosecution or punishment of breaches of the law which impose penalties or sanctions;
- preparation for proceedings before any court or tribunal;
- conduct of proceedings before any court or tribunal; and
- implementation of the orders of a court or tribunal.

Where personal information is used or disclosed in reliance on the above, the department will record a note of the use or disclosure on the relevant record.

Permitted non-compliance for law enforcement functions

Section 29 of the IP Act permits a law enforcement agency to not comply with certain privacy principles in specific circumstances. In these circumstances, the department does not have to comply with:

- IPP2: provide a collection notice
- IPP3: only collect relevant, complete and up to date personal information, and do not intrude unreasonably on an individual's personal affairs
- IPP9: only use relevant personal information
- IPP10: only use personal information for the purpose for which it was collected, unless an exception applies
- IPP11: do not disclose personal information to anyone but the individual it is about, unless an exception applies.

There are a number of criteria, set out in the subsections to section 29 which must be met before a law enforcement agency can rely on section 29.

When do the privacy principles not apply?

In some circumstances, the IP Act recognises that it is appropriate to create a number of exceptions to and exemptions from the obligation to comply with the IPPs. Schedule 1 of the IP Act sets out the documents to which the privacy principles do not apply:

- Covert Activity—specified documents containing personal information arising out of, or in connection with, certain activities under the *Police Powers and Responsibilities Act 2000* or the *Crime and Corruption Act 2001,* or of a law enforcement agency, or obtained under a warrant issued under the *Telecommunications (Interception and Access) Act 1979* (Cwlth).
- Witness protection—documents containing personal information about a witness who is included in a witness protection program under the *Witness Protection Act 2000* or who is subject to other witness protection arrangements made under an Act.
- Disciplinary actions and misconduct—documents containing personal information about an individual arising out of a complaint made under Part 7 of the *Police Service Administration Act 1990* or an investigation of police misconduct or corrupt conduct under the *Crime and Corruption Act 2001.*
- Public Interest Disclosure—documents containing personal information about an individual that is contained in a public interest disclosure or personal information that has been collected in an investigation arising out of a public interest disclosure under the *Public Interest Disclosure Act 2010*.
- Cabinet and Executive Council documents—A document to the extent it contains personal information that is also the subject of the *Right to Information Act 2009*, schedule 3, sections 1, 2 or 3.
- Commissions of Inquiry—documents containing personal information about an individual arising out of a commission of inquiry.
- Reference and study documents—a document kept in a library, art gallery or museum for the purposes of reference, study or exhibition.
- Public records—a public record under the *Public Records Act 2002* in the custody of Queensland State Archives that is not in a restricted access period under that Act.
- Postal material—a letter, or anything else, whilst being transmitted by post.

Although these documents may not be subject to the IPPs, these documents may have secrecy or confidentiality obligations set out in other relevant legislation.

Transfer of personal information outside Australia

In addition to the 11 IPPs, the department abides by section 33 of the IP Act when managing personal information.

Section 33 of the IP Act sets out the limited circumstances when an agency may transfer personal information outside of Australia. Outside of express consent, legislative authority or serious health and safety benefits, the agency must satisfy requirements to ensure the protection of that information. In summary, when transferring personal information to an overseas cloud hosting facility, the department ensures that the vendor will manage the personal information in accordance with the whole of

government ICT-as-a-service offshore data storage and processing policy and in a manner consistent with the IPPs.

Section 33 of the IP Act sets out four circumstances in which a transfer of personal information outside of Australia may occur:

33(a) – the individual has agreed

33(b) – the transfer is authorised or required under a law

33(c) – the agency is satisfied on reasonable grounds that the transfer is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of any individual, or to public health, safety and welfare

33(d) – if two or more of the criteria in 33(d) apply:

(i) the recipient of the personal information is subject to equivalent privacy obligations

(ii) transfer is necessary to perform a function

(iii) transfer is for the individual's benefit

(iv) reasonable steps have been taken to ensure the personal information is protected.

The department ensures that appropriate privacy assessments are conducted prior to the transfer of personal information outside of Australia.

Information Technology

Social Media

The department has established official accounts on Facebook and Twitter to reach and engage with audiences within the community. Any information provided on the department's social media sites will only be used to perform our functions or activities. The department will not send personal details to any third parties without the individual's consent, unless required or authorised to do so by law. Users of these accounts must be aware of the individual social media site's terms of use and privacy conditions prior to use.

Topics that can be expected to be found on the department's Facebook and Twitter accounts include:

- safety messages and tips
- updates on projects/initiatives/services
- infrastructure milestones
- announcing new development technologies or innovations
- community consultation opportunities
- emergency information.

Mobile Apps

Mobile applications or ‘apps’ are software programs designed to run on a smartphone, tablet computer or other mobile device. The department currently has a range of mobile apps that are capable of capturing personal information such as location, device or contact details. Personal Information that is collected via applications are only used by the department for the purpose it was collected and managed in accordance with the IPPs.

Cloud Computing

Cloud computing is a term for moving functions from a computer and agency-owned server to an online environment, usually as a solution for the storage, management, and processing of data. Sometimes cloud computing servers are located outside of Australia, and as a result, personal information is transferred overseas. The department will manage the personal information in accordance with the whole of government ICT-as-a-service offshore data storage and processing policy.

CCTV

The department uses CCTV (closed-circuit television) systems in many locations throughout Queensland, primarily for safety and security purposes and for monitoring and managing transport operations and road systems.

Some examples of CCTV usage within the department include:

- maintaining security of workplaces or sites
- observing driver behaviour
- observing passenger/customer behaviour (e.g. TransLink Busways)
- traffic monitoring
- building, facilities and construction site security
- obtaining a visual record of activities in situations where it is necessary to maintain proper security or monitoring (e.g. Customer Service Centres).

Any time a CCTV captures pictures or video footage of an identifiable individual, it is potentially capturing personal information. The department’s CCTV systems are operated with respect for people's privacy, and the images captured by the CCTV are maintained in the following manner:

- recording and retention of images are undertaken fairly and lawfully
- recorded images are only used for the purpose for which the CCTV system was installed, unless these images are required by a law enforcement agency
- individuals are made aware through various mechanisms that they are subject to CCTV surveillance, unless the system is being used for investigation or other law enforcement purposes.

Body Worn Cameras

The department's compliance officers, which include Transport Inspectors, Maritime Officers and TransLink's Senior Network Officers use body worn cameras.

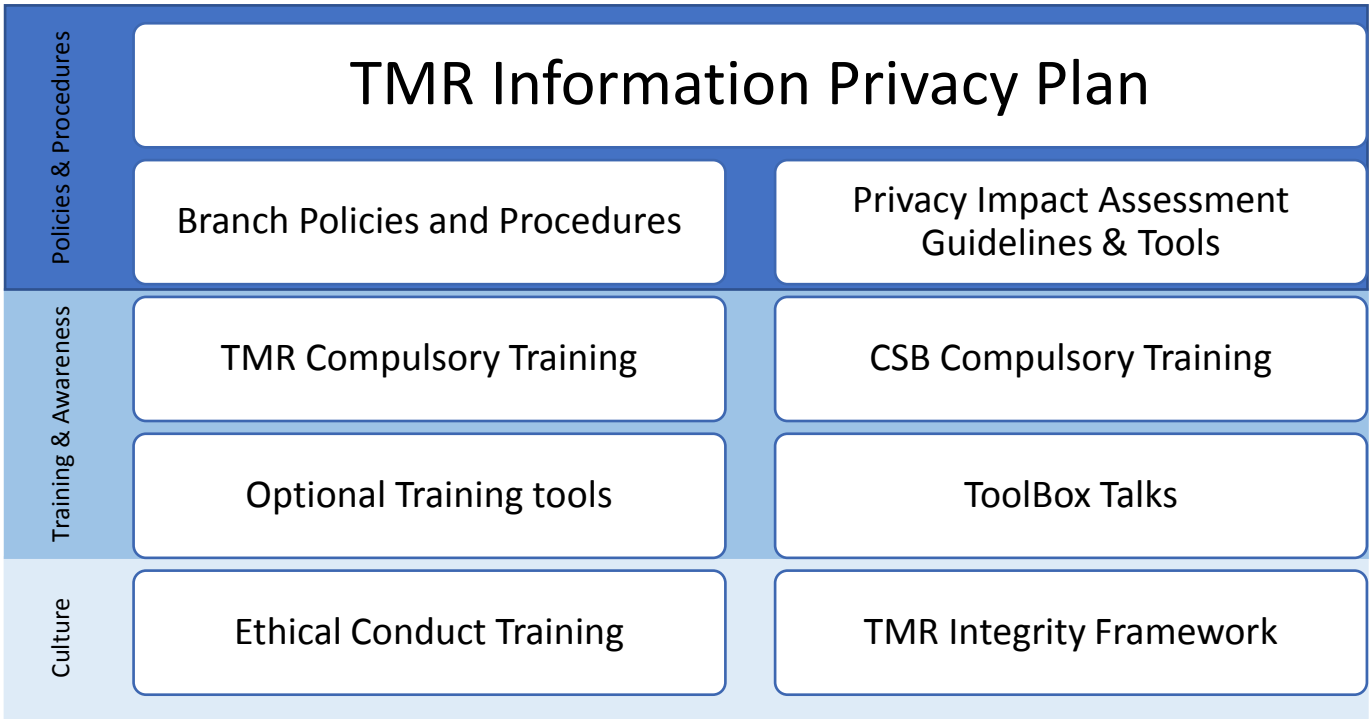
Body Worn Cameras (BWCs) are becoming an increasingly valuable tool for law enforcement agencies around the world and throughout Australia. In implementing this technology there are vast benefits to be gained; of particular note is the important step towards transparent and effective compliance enforcement.

Implementation of BWCs in law enforcement agencies have demonstrated benefits from using BWCs integrated with a digital evidence management system including:

- improvements in customer experience;
    - as both the Queensland Government employee and the member of the public behave in a more positive manner;
    - through a reduction in response time for complaint management, as accessibility to image and voice data reduces the time associated with investigating complaints
- efficiency improvements in the digital evidence management workflow
- decreasing complaints against compliance officers
- reducing the number of unsuccessful matters brought before the court; and
- reducing assaults against compliance officers.

The department is conscious of respecting people's privacy, as such its compliance officers will only activate body worn camera video recording when exercising a power. This approach will reduce capturing the personal information of customers not involved with the enforcement action.

TMR Information Privacy Framework



Roles and Responsibilities

An effective privacy governance framework benefits everyone and begins with the department's leadership. The framework helps clarify each person's role in effective privacy management and ensures that they are held to account. With appropriate and adequate policies, processes and reporting in place, privacy management ensures a seamless integration into business as usual practices. This framework will also help foster a culture of viewing privacy as the department asset amongst employees.

Effective privacy compliance implementation includes the following key functions and roles:

Director- General

The Director-General is the accountable officer for ensuring the department's administrative procedures and management of information practices adhere with privacy obligations.

Governance Branch

The department's Governance Branch, Corporate Division, is responsible for ensuring and managing privacy compliance, reporting and providing advice to members of the public and employees about the department's privacy obligations including:

- ensuring employees have access to adequate training materials in relation to privacy compliance
- assisting in responses to and reporting of complaints and breaches of privacy
- assisting business units in conducting privacy impact assessments when designing and implementing new projects and programs that involve the management of personal information

- conducting self-compliance assessments on all datasets that hold personal information
- maintaining and periodically reviewing the TMR Information Privacy Plan.

General Managers

The department's General Managers are committed to transparency and accountability in respect of the department's compliance with the IP Act across their business unit activities (projects, programs and service delivery) by:

- ensuring Policies and Procedures are in place to maintain to uphold the IPPs
- ensuring employees are educated about the privacy compliance obligations
- referring complaints/breaches to the Governance Branch
- seeking advice when considering new projects or programs that involve the management of personal information.

Employees, contractors and consultants to the department

All employees, contractors and consultants within the department have an accountability to ensure that the personal information they handle is managed in accordance with the relevant policies and procedures set by the department to ensure privacy compliance, including reporting breaches of privacy.

The department regularly engages external entities to perform some of its functions or activities. This process of contracting out services or functions to an external provider is referred to as “outsourcing.”

Where these arrangements require access to, or collection of personal information on behalf of the department, the IP Act requires that all reasonable steps are taken by the department to ensure that these service providers are bound to comply with the IPPs and section 33 of the Act which relates to the transfer of personal information outside of Australia.

There is a variety of resources on the department's intranet to assist employees and contractors learn about their privacy obligations. All employees and contractors of the department are required to complete online privacy awareness training upon induction, with a further refresher required every two years. The online training program provides employees and contractors with an overview of what is expected when managing the personal information of individuals and their co-workers.

Ethical Standards Unit

The role of the department's Ethical Standards Unit (ESU) is to discharge statutory obligations imposed on the Director-General to notify the Crime and Corruption Commission (CCC) of suspected corrupt conduct.

In all instances whereby alleged breaches of privacy involve alleged serious misconduct or corrupt conduct, the matter is to be referred to the ESU. The ESU will undertake an assessment and determine whether the matter is dealt with in accordance with the Public Service Commission Conduct and Performance Excellence (CaPE) Framework or requires notification to the Crime and Corruption Commission. The ESU will manage investigations involving alleged serious misconduct or corrupt conduct.

Audit and Risk

The role of Internal Audit and Risk is to assist the Director–General in arriving at the most appropriate treatment for risks and then monitoring and reviewing the risks and controls. This includes oversight of the integrity of the department's internal controls such as:

- compliance with legislative and regulatory requirements
- the process relating to internal risk management and control systems
- the performance of the internal audit function.

Information Privacy Breach

A privacy breach is defined as “unauthorised access to or disclosure of personal information, or a loss of personal information”. Privacy breaches can occur because of a technical problem, human error, inadequate policies and training, a misunderstanding of the law, or a deliberate act. Some of the more common privacy breaches happen when personal information is lost, stolen or accidently disclosed.

In the event that the department does experience a privacy breach, or suspects that a breach has occurred, a privacy breach repsonse plan is referred to, enabling the department to contain and assess the breach, and respond in a timely manner. This helps minimise potential damage to both the individual and the department .

The four key steps considered when responding to a privacy breach include:

- containing the breach
- evaluating the associated risks
- consider notifying affected individuals
- how to prevent a repeat

Whilst breach notification is not mandated under the IP Act, it is recognised that effective breach management, including notification where warranted, will assist in avoiding or reducing possible harm to both the affected individuals and the department.

Suspected Misuse of Personal Information

If someone suspects or becomes aware of a privacy breach, it should immediately be reported to the department’s RTI, Privacy and Complaints Management Unit. A Privacy Breach Notification Form will be provided to the business area where the privacy breach occurred, unless the circumstances indicate the breach should first be referred to the ESU. This form should be completed as soon as possible and submitted via email to privacy@tmr.qld.gov.au for assessment

Where any suspected or known privacy breach can be contained by taking immediate steps to limit any further access or distribution of the affected personal information, these steps should be taken. Such action is not appropriate if it would compromise or destroy evidence that may be valuable in identifying the cause of the breach.

On receiving a Privacy Breach Notification Form, or otherwise being notified of a suspected breach, the RTI, Privacy and Complaints Management Unit will record the incident and undertake an assessment of the incident. Consideration will be given as to the type of personal information involved

in the breach, the circumstances of the breach, including its cause and extent; the nature of the harm to affected individuals, and if this harm can be removed through remedial action.

In instances whereby a suspected breach of privacy may involve alleged serious misconduct or corrupt conduct, the ESU will undertake an assessment and determine whether the matter is dealt with in accordance with CaPE Framework or requires notification to the Crime and Corruption Commission (CCC).

Recommendations as to how any notification is conducted as well as draft recommendations addressing the department's ongoing review of the incident to improve its personal information handling practices will be provided by the RTI, Privacy and Complaints Management Unit to the relevant business areas for actioning.

Information Privacy Complaints

If an individual believes that the department has not dealt with their personal information in accordance with the requirements set out in the IP Act, they may submit an information privacy complaint.

A privacy complaint is a complaint by an individual about an act or practice of a department in relation to the individual's personal information.

Privacy complaints made to the department must:

- include an address of the complainant to which notices may be forwarded under the IP Act
- provide certified identification
- give particulars of the act or practice which is the subject of the complaint.

Privacy complaints may be marked Private and Confidential and forwarded to:

RTI, Privacy and Complaints Management
Department of Transport and Main Roads
GPO Box 1549
Brisbane Qld 4001

Complaints will be acknowledged in writing within 14 days from the date on which the complaint is received and processed within 45 business days.

In the circumstance where a longer period of time is required in order to finalise a complaint, the complainant will be contacted with a view to keeping the complainant informed of progress.

On completion, the complainant will be advised in writing of the department's decision, including any remedies that are considered appropriate to resolve the complaint.

For general privacy enquiries, the department's RTI, Privacy and Complaints Management Unit can be contacted via phone on (07) 3066 7108. General enquiries can also be made via email to privacy@tmr.qld.gov.au.

Mediation by the Office of the Information Commissioner

If a complainant does not agree with the department's decision or the action taken to address a complaint, they may refer their matter to the Office of the Information Commissioner (OIC) after 45 business days has lapsed from the date the complaint was received by the department.

The OIC is an independent statutory body established under the *Right to Information Act 2009* (QLD) to endeavour to resolve privacy complaints made after 2009, where the complainant has previously lodged a complaint with a government agency but remains dissatisfied with the outcome of that process.

Complaints to the Office of the Information Commissioner must be made in writing either by completing a hard copy of the complaint form contained on the website http://www.oic.qld.gov.au, or by letter, to the OIC office at:

Office of the Information Commissioner

PO Box 10143, Adelaide St

Brisbane QLD 4000

telephone: 07 3234 7373 or 1800 642 753

email: administration@oic.qld.gov.au

For More Advice

The RTI, Privacy and Complaints Management Unit is the first point of contact for members of the public and employees on privacy matters, including:

- compliance and general information on privacy in the department
- requests to amend records containing personal information
- privacy impact assessments for new projects or programs
- suspected breaches and privacy complaints
- conducting and reviewing results of information privacy assessments
- training and awareness material.

The RTI, Privacy and Complaints Management Unit can be contacted at privacy@tmr.qld.gov.au or by phoning (07) 3066 7108.