

Department of Community Safety

***Information
Privacy
Plan***

2009

Prepared by:
Information Rights Unit
Strategic Policy Division
Department of Community Safety

This document has been prepared with all due diligence and care, based on the best available information at the time of publication. The department holds no responsibility for any errors or omissions within this document. Any decisions made by other parties based on this document are solely the responsibility of those parties. Information contained in this document is from a number of sources and, as such, does not necessarily represent government or departmental policy.

September 2009
Version 1.0

Foreword

Under the *Information Privacy Act 2009* and the *Right to Information Act 2009* the department is responsible for ensuring personal information holdings are appropriately managed and protected.

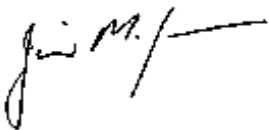
The Information Privacy Plan is a tool in this process and is designed to assist with understanding how we manage personal information and how we afford privacy rights with respect to our activities.

The Plan describes classes of personal information held, how the information is used and how individuals can access and amend their personal information. It also describes the Agency's complaint handling process which is available for individuals who believe their privacy has been breached.

Because of the type of duties performed by the Agency we must be sensitive to privacy issues and treat seriously the ongoing trust the community has placed in us to administer our affairs with due diligence and in accordance with Government legislation and policy.

Adhering to the privacy requirements will help us in our commitment to continue to provide an efficient and effective world standard community safety agency.

I encourage you to make use of the Information Privacy Plan and welcome any feedback which should be directed to the privacy contact officer on (07) 3405 6283 or by email at privacy@dcs.qld.gov.au



JIM MCGOWAN
Director-General
Department of Community Safety

Contents

Introduction	5
Personal Information	5
What is personal information?	5
What is not personal information?	6
Exempt personal information	6
Covert activity	6
Witness protection	6
Disciplinary actions and misconduct	6
Whistleblowers	6
Cabinet and Executive Council documents	6
Commissions of inquiry	6
Other	6
Summary of the information privacy principles	6
Information Privacy Principles	7
Application of this plan	7
Departmental employees	7
Contractors and consultants to the department	7
Joint venture partners	7
Responsibilities of privacy in the Department of Community Safety	8
Classes of personal information held	8
Employee personal records	8
Personnel and payroll	8
Recruitment	8
Other records	9
Financial Management Records	9
Information Systems Records	10
Ministerial Correspondence	10
Administration Records	11
Custodial Operations Records	11
Probation and Parole (Community Corrections) Records	12
Community Supervision	12
Parole Board Records	13
Intelligence and Investigation Records	14
Right to Information, Privacy, Judicial Review and Litigation Records	15
Victims Register	15
Official Visitor Records	16
Ambulance Records	16
Public registers managed within the Department	16
Access and amendment procedures	17
Complaint and Review Process	17
Acts administered by the Department of Community Safety	17
Appendix 1 - Information Privacy Principles	19
Information Privacy Principle 1	19
Information Privacy Principle 2	19
Information Privacy Principle 3	19
Information Privacy Principle 4	20
Information Privacy Principle 5	20
Information Privacy Principle 6	20
Information Privacy Principle 7	20
Information Privacy Principle 8	21
Information Privacy Principle 9	21
Information Privacy Principle 10	21
Information Privacy Principle 11	21

Introduction

Privacy is about protecting the personal information of individuals. The *Information Privacy Act 2009* provides for access and amendments rights for personal information held by the Government.

Obligations about the collection, use, storage and disclosure of personal information are provided in the Information Privacy Principles now included in the *Information Privacy Act 2009*.

These Information Privacy Principles were originally contained within Information Standard 42 - Information Privacy (IS42). IS42 has now been superseded by the *Information Privacy Act 2009*.

The 11 Information Privacy Principles established under IS42 have been reworded but retained in Schedule 3 of the *Information Privacy Act 2009*.

Under the *Information Privacy Act 2009*, personal information held by Queensland Government agencies must be responsibly and transparently collected and managed (including transfer of personal information held by agencies to other agencies, other levels of Government or the private sector) in accordance with the requirements of the Information Privacy Principles.

The *Information Privacy Act 2009* also provides a new complaints mechanism for any act or practice that is a breach of the Information Privacy Principles. Breaches of the Act can result in penalties of up to \$100,000 in compensation being awarded by the Queensland Civil and Administrative Tribunal (QCAT).

The aim of this plan is to assist members of the public to understand how personal information is managed within the department and how they can seek assurance that their personal information is maintained in accordance with the *Information Privacy Act 2009*.

It will also serve as guidance for employees who deal with personal information and will provide a strategic overview for achieving compliance by the department with the *Information Privacy Act 2009*.

Personal Information

What is personal information?

For the purposes of identifying information to be managed in accordance with this information privacy plan, personal information is defined as any information that would allow a person to be identified.

Personal information is defined in the *Information Privacy Act 2009* 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.

Examples include a person's name and address, signature, email address, date of birth, drivers licence number, physical characteristics such as height, birthmarks, tattoos, and psychological profiles.

It also includes sensitive information such as political and religious beliefs, medical records, disabilities and sexual preferences.

The information does not have to clearly identify a person. It need only provide sufficient information to lead to the identification of a person. It is not limited to confidential or sensitive personal details. It covers information held in paper or electronic records, including images and sounds.

What is not personal information?

Personal information does not apply to information in publications that are generally available. Generally available publications include documents such as magazines, books, a newsletter or a newspaper article, annual reports and the Queensland Government Gazette.

Exempt personal information?

The following personal information is exempt from the *Information Privacy Act 2009*:

Covert activity

- personal information about an individual arising out of or in connection with a controlled operation or controlled activity within the meaning of the *Police Powers and Responsibilities Act 2000*;
- personal information about an individual arising out of or in connection with a covert undertaking of an operation, investigation or function of a law-enforcement agency;
- personal information about an individual arising out of a warrant issued under the *Telecommunications (Interception) Act 1979* of the Commonwealth.

Witness protection

Personal information about a witness who is included in a program under the *Witness Protection Act 2000*, or who is subject to other witness protection arrangements made under an act.

Disciplinary actions and misconduct

- personal information about an individual arising out of a complaint made under Part 7 of the *Police Service Administration Act 1990*; and
- personal information about an individual arising out of an investigation of misconduct or official misconduct under the *Crime and Misconduct Act 2001*.

Whistleblowers

Personal information about an individual that is contained in a public interest disclosure within the meaning of the *Whistleblowers Protection Act 1994*, or that has been collected in the course of an investigation arising out of a public interest disclosure.

Cabinet and executive council documents

Personal information about an individual that is contained in a cabinet or executive council document that is also the subject of the *Right to Information Act 2009*, schedule 3, section 1, 2 or 3.

Commissions of inquiry

Personal information about an individual arising out of a commission or inquiry.

Other

Additionally, the IPPs do not apply where the:

- authority to collect, use, store and disclose personal information has an overriding statutory base;
- personal information concerns a deceased person; and
- personal information is in a publicly available document.

Summary of the information privacy principles

There are 11 Information Privacy Principles (IPPs). These principles have been adapted from the *Commonwealth's Privacy Act 1988* and:

- cover the way the Department of Community Safety will collect, store, use and disclose personal information about people;

- allow people access to their personal information held by the department; and
- allow people to request changes or amendments to this information.

The Department of Community Safety must comply with 11 IPPs, which govern how personal information is collected, stored, used and disclosed.

Information Privacy Principles (IPPs):

- Principle 1: Collection of personal information (lawful and fair);
- Principle 2: Collection of personal information (requested from individual);
- Principle 3: Collection of personal information (relevance, etc);
- Principle 4: Storage and security of personal information;
- Principle 5: Providing information about documents containing personal information;
- Principle 6: Access to documents containing personal information;
- Principle 7: Amendment to documents containing personal information;
- Principle 8: Checking of accuracy, etc. of personal information before use;
- Principle 9: Use of personal information only for relevant purpose;
- Principle 10: Limits on use of personal information;
- Principle 11: Limits on disclosure of personal information.

Application of this plan

The Department of Community Safety's information privacy plan applies to:

- departmental employees;
- volunteers;
- contractors and consultants to the department; and
- joint venture partners.

Departmental employees

When dealing with personal information, Department of Community Safety's employees will comply with the information privacy principles outlined in this plan.

Contractors and consultants to the Department

The Department of Community Safety regularly enters into contracts with external bodies for the supply of goods and services. Some of these contracts require the disclosure of personal information to third parties, or the collection of personal information by third parties on behalf of the department.

The *Information Privacy Act 2009* requires personal information to be managed in accordance with the Information Privacy Principles and that any outsourcing arrangements, contracts and licenses entered into after 1 July 2009 must comply with these principles.

It should be noted that existing outsourcing arrangements, contracts and licenses entered into prior to July 2009 will remain in force and comply with IS42.

Joint venture partners

Where the Department of Community Safety has partnership agreements with companies or individuals, such agreements will comply with the *Information Privacy Act 2009* when entering into a new contract or renewal.

Responsibilities for privacy in the Department of Community Safety

The overall responsibility for privacy in the Department of Community Safety rests with the Director-General. All staff within the Department of Community Safety have a responsibility to ensure they comply with the *Information Privacy Act 2009*.

The day-to-day management of privacy has been delegated to the Information Rights Unit. The Manager Information Rights Unit is the first point of contact for members of the public and employees on privacy matters, including:

- breach of privacy complaints;
- requests for internal reviews;
- requests to amend records; and
- general information on privacy in the Department of Community Safety.

The Manager Information Rights Unit can be contacted at privacy@dcs.qld.gov.au or by phone on (07)323 93695.

The Information Rights Unit is also responsible for reporting privacy matters to the Director-General and for preparing relevant statistical reports for senior management.

Classes of personal information held

The Department of Community Safety holds a range of information on employees that falls within the definition of personal information.

Employee personnel records

- personnel and payroll;
- recruitment; and
- other records.

Personnel and payroll

The records may include details about:

- attendance and overtime;
- leave applications and approvals;
- medical records;
- payroll and pay, including banking details;
- tax file number declaration forms;
- declarations of pecuniary interests;
- personal history files;
- education;
- performance appraisals, etc;
- personal development and training;
- trade, skill and aptitude tests;
- completed questionnaires and personnel survey forms;
- removals;
- travel documentation;
- personal welfare matters; and
- contracts and conditions of employment.

Recruitment

The records may include details about:

- recruitment;
- relocation of staff and removals of personal effects; and
- character checks, security clearances and criminal history checks.

Other records

The records may include detail about:

- accidents and injuries, including compensation and rehabilitation case files;
- counselling and discipline matters, including disciplinary, complaints, grievances, investigation and action files, records of criminal convictions, and any other staff and establishment records as appropriate;
- recommendations for honours and awards; and
- any CCTV photographic imagery retained for employee and public safety purposes.

Content may include: name, address, date of birth, occupation, employee identification number, gender, qualifications, equal employment opportunity group designation, next of kin, details of pay and allowances, leave details, work reports, security clearances, criminal history checks and employment history.

Sensitive content may include details of: physical and mental health, disabilities, racial or ethnic origin, disciplinary investigation and action, criminal convictions, adverse performance and security assessments, tax file numbers, relationship details and personal financial information.

Any CCTV photographic imagery that is taken in the act of providing employee and public safety measures will be retained only in electronic form. These records will be accessed only as required by an authorised officer.

The following staff have access to this personal information subject to appropriate security authority and operational need: personnel management staff; supervisors and members of selection committees (if appropriate); and the individual to whom the record relates.

Some personal information may also be accessed by contracted private companies or government agencies, such as the Department's shared service provider, SSA, in order to provide services, or to support and maintain human resource databases.

Personnel records are kept for variable periods according to the applicable provisions of the general retention and disposal schedule for staff and establishment records issued by Queensland State Archives.

Some of this information may be disclosed to: the Australian Taxation Office, QSuper, Public Service Commission and to third parties such as banks and insurance companies (name and account numbers only), where legally required.

Current and former employees and other persons (for example, spouses and next of kin who believe that the Department's personnel records may also contain personal information about them) can obtain details of specific record handling practices of particular business areas by contacting supervisors in those business areas.

Records relate to all current and former employees of the Department and are stored on paper and electronic media.

Individuals can obtain information regarding access to their personal information by contacting the Manager, Information Rights Unit, email privacy@dcs.qld.gov.au or phone (07)323 93695.

Financial Management Records

The purpose of these records is to process and account for expenditure and revenue. There is commonality amongst these records across various business areas of the Department, so they are grouped here as one entry.

Content may include: name, address, service or goods category, bank account details and transaction history.

Sensitive content may include: financial information concerning creditors and debtors (including engaged service providers if they are identified personally).

The following staff have access to this personal information subject to appropriate security authorisation and operational need: finance administration staff (central and relevant business area) within the Department.

Some personal information may also be accessed by contracted agencies, such as the Department's shared service provider, SSA, in order to provide services such as account and payroll processing or to support and maintain financial systems databases.

The records are kept according to the categories set out in the general retention and disposal schedule issued by Queensland State Archives.

This information is not usually disclosed to other persons or organisations. The records are stored on paper and electronic media.

Individuals can obtain information regarding access to their personal information by contacting the Manager, Information Rights Unit, email privacy@dcs.qld.gov.au or phone (07)323 93695.

Information Systems Records

The Department's information management systems network routinely carries, enables processing of, and stores, for varying periods, much of the core business and the supporting corporate service business of the Department including the majority of personal information records described within this plan. Some information systems for human resource and finance functions are also provided by the Department's shared service provider, SSA.

Content may include: name, address, passwords, internal electronic transactions and external transactions, telephone numbers, e-mail (including individual and whole of department e-mail address groups), internet and government intranet activity.

Sensitive content may include details of: personal e-mail messages and address books, information technology system security identifiers and passwords and staff internet usage tracking records.

The following departmental staff have access to the personal information subject to appropriate security authorisation and operational need: staff supervisors, system administrators and the individual staff member concerned. Staff are routinely made aware of system usage rules and monitoring procedures concerning collection and use of the information.

The records are retained as provided for under the general retention and disposal schedule authorised by Queensland State Archives.

The information is not usually disclosed to persons outside the Department. The records are stored on paper and electronic media.

Individuals can obtain information regarding access to their personal information by contacting the Manager, Information Rights Unit, email privacy@dcs.qld.gov.au or phone (07)323 93695.

Ministerial Correspondence

Inwards correspondence, addressed to the Minister or the Minister's office staff, from the public or other government agencies on a wide array of matters of official business of the Minister's portfolio, may be referred to the Department for consideration and preparation of advice and responses including outward correspondence.

Content may include: names, addresses, personal opinions about public administration matters, occupational and organisational information about persons, complaints and grievances and any other matter that the correspondent wishes to convey to the Minister about themselves or personally identifiable third parties in government or amongst the public.

Sensitive content may include details of: physical and mental health, racial or ethnic origin, disciplinary investigations and action, criminal convictions, relationships and allegations of wrongdoing.

The following departmental staff have access to some of this personal information subject to appropriate security authorisation and operational need: executive and senior staff, administrative staff who process the correspondence and other departmental staff in order to respond to the correspondence.

The records under the control of the Department containing the personal information are retained for periods provided for under the general retention and disposal schedule authorised by Queensland State Archives.

The information is not usually disclosed to other persons or organisations. The records are stored on paper and electronic media and may include photographic images.

Individuals can obtain information regarding access to their personal information in ministerial correspondence records held by the Department, by contacting the Manager, Information Rights Unit, email privacy@dcs.qld.gov.au or phone (07)323 93695.

Administration Records

Administration records support the objectives of the Department by assisting with the effective and efficient operation of all areas of the Department. The records related to correspondence, policy and program drafting and development, mailing lists, purchasing, stakeholder groups, communication and publications, audit outcomes, security and general management issues.

Content may include: name, home address, e-mail account, date of birth, gender, telephone numbers, car pool registers, public relations detail.

Departmental staff have access to this information subject to appropriate security authorisation and operational need including authorised IT systems administration staff.

The records are retained as provided for under the general retention and disposal schedule authorised by Queensland State Archives.

The information is not normally disclosed to other persons or organisations without the consent of the person about whom the personal information relates, or if a statutory or contract obligation exists.

The records are generally stored on paper and electronic media. The records may include videotape, audiotape and photographic images.

Individuals can obtain information regarding access to their personal information from the Manager, Information Rights Unit, email privacy@dcs.qld.gov.au or phone (07)323 93695.

Custodial Operations Records

Correctional services provide for the management of adult prisoners in thirteen centres throughout the State including three open custody facilities and two centres under the management of engaged service providers.

Custodial Operations records relate to all prisoners in custodial operations facilities, including prisoner health and medical records and visitor records. The purpose of the records is to assist in the management of all aspects of a prisoner's time in custody.

The Brisbane Women's Correctional Centre (BWCC) Program comprises Helana Jones Centre and the Warwick work camp for women. A supportive environment for women prisoners (some with their young children) is provided to assist them to rehabilitate and reintegrate into the community.

Content may include: name, address, date of birth, gender, physical description, education, financial details, prisoner identification number and photograph, programs performance and custodial conduct, health data, applications to visit, visitor details, employment information, next of kin and family member information.

Sensitive content may include: physical and mental health, racial or ethnic origin, criminal and offending history, current personal circumstances, religious affiliation, relationship and family details, bank and

trust account details, visitor criminal history checks, results of searches and strip searches, electronic monitoring and surveillance, mail and telephone monitoring details.

The following Agency staff have access to some of this personal information subject to appropriate security authorisation and operational need: senior management and staff in the Agency and the custodial facility, sentence management staff, staff of service providers contracted to Agency as well as authorised IT systems administration staff.

The records are retained as provided for under the Agency's retention and disposal schedule authorised by Queensland State Archives. Paper based records are kept at the facility where the offender is currently held. Surveillance videotapes are reused regularly unless required to be kept as evidence. Some electronic data (such as bed assignment) is deleted on discharge of the offender.

Some of this information may be disclosed to the offender's legal representatives, registered persons on the Victims Register, other government Departments where statutory obligations exist (ie Commonwealth Department of Immigration and Ethnic Affairs and Attorney-General, Centrelink, law enforcement agencies and the courts), the Crime and Misconduct Commission, the Ombudsman, foreign consulates Official Visitors and Parole Board members, and external researchers under agreement or contract.

The *Corrective Services Act 2006* also recognises the culturally specific needs of Aboriginal and Torres Strait Islander (ATSI) offenders. Disclosure of information to the wider family unit and traditional elders may be made to ensure the health and well being of ATSI offenders.

Individuals can obtain information regarding access to their personal information from the *Information Privacy Act 2009* or the Information Rights Unit, email privacy@dcs.qld.gov.au or phone (07)323 93695.

The records are generally stored on paper and electronic media. The records may include videotape and audiotape, photographic images and biometric data.

Locations: Lotus Glen Correctional Centre (near Mareeba); Townsville Correctional Centre; Townsville Women's Correctional Centre; Capricornia Correctional Centre (near Rockhampton); Woodford Correctional Centre (near Caboolture); Brisbane Correctional Centre (Wacol); Brisbane Women's Correctional Centre (Wacol); Wolston Correctional Centre (Wacol); Arthur Gorrie Correctional Centre (engaged service provider-Wacol); Borallon Correctional Centre (engaged service provider-near Esk); Darling Downs Correctional Centre (near Toowoomba); Palen Creek Correctional Centre (near Rathdowney); Numinbah Correctional Centre (Gold Coast hinterland); and Maryborough Correctional Centre.

Archived custodial offender files are managed by Records Management Central Archives, Wacol.

Probation and Parole (Community Corrections) Records

The role of community corrections is to assist courts and community corrections boards in assessing offenders' suitability for community placement and, once offenders are placed in the community, to enforce court or board orders, protect the community, assist offenders to change and support the rights of their victims.

The Probation and Parole Directorate in Central Office is responsible for community facilities operated by the Agency, including regional and area offices.

Community Supervision

The majority of offenders in the care of the Agency are managed through supervision provided in the community. Eight regions are responsible for 35 district offices throughout Queensland.

Community supervision manages offenders released from custody on parole orders and also offenders who have not been sentenced to imprisonment, but are supervised in the community under a court order. Court orders include intensive correction, intensive drug rehabilitation, probation, community service, intensive correction order, supervision orders and fine option orders. Offender management records are held for all offenders in probation and parole facilities.

Content of the records may include: name, address, date of birth, gender, physical description, education, financial details, court order/s, results of breaches of discipline and involvement in incidents, offender identification number and photograph, community service and employment performance and conduct, financial and property advice and probation and parole orders, next of kin and family member information.

Sensitive content may include details of: physical and mental health, racial or ethnic origin, criminal and offending history, current personal circumstances, religious affiliation, relationships and families, bank and trust accounts, results of previous supervision orders, performance in custody, results of searches, results of board deliberations on applications for post-prison release, and name and location of employer and community service provider.

The following Agency staff have access to some of this personal information subject to appropriate security authorisation and operational need: senior management and staff in area offices and corrections facilities, particularly the district manager or supervising officer of the offender, sentence management staff and Parole Boards and authorised IT systems administration staff. All authorised Agency staff have electronic access to the personal information.

Offender management records are maintained at all probation and parole operational sites where the offender is held or in the district office to which the offender reports or reported. When an offender is discharged some records may also be sent to archives. The records are kept in accordance with the Agency's retention and disposal schedule authorised by Queensland State Archives.

Some of this information may be disclosed to: the offender's legal representatives, registered persons on the Victims Register, other government Departments where statutory obligations exist (ie Commonwealth Department of Immigration and Ethnic Affairs and Attorney-General, Centrelink, law enforcement agencies and the courts), the Ombudsman, foreign consulates, Parole Board members and external researchers under agreement or contract.

The Act recognises the culturally specific needs of Aboriginal and Torres Strait Islander (ATSI) offenders. Disclosure of information to the wider family unit and traditional elders may be made to ensure the health and well being of ATSI offenders.

Individuals can obtain information regarding access to their personal information from the Manager, Information Rights Unit, email privacy@dcs.qld.gov.au or phone (07)323 93695.

The records are generally stored on paper and electronic media. The records may include videotape and audiotape, photographic image, biometric data and body samples.

Location: Probation and Parole Directorate in Central Office, regional offices, district offices, and the Parole Boards Secretariat. In addition, there is one contract managed community corrections centre and two contract managed indigenous community corrections centres.

Parole Board Records

The Parole Boards are statutory bodies primarily responsible for making decisions with respect to the release of prisoners on post-prison community based release orders and for reviewing prisoners' progress whilst on post-prison community based release orders. Support to the Boards is provided by the Agency.

The purpose of Board records is to enable the Boards to properly exercise their functions outlined in chapter five of the *Corrective Services Act 2006*.

Content may include: name, address, date of birth, gender, physical description, education, criminal history, programs performance and custodial conduct.

Sensitive content may include: physical and mental health, racial or ethnic origin, criminal and offending history, current personal circumstances, relationship and family details, attitude towards victims of crime, Board deliberations on applications for post-prison release.

The following Agency staff have access to this personal information subject to appropriate security authorisation and operational need: senior management and staff in district offices and correction

facilities, sentence management staff, the district manager or supervising officer, board members and secretariats and authorised IT systems administration staff.

The records are generally kept in the Boards' Secretariat. Some records may be stored for archival purposes with Ausdoc. The records are kept in accordance with the general retention and disposal schedule authorised by Queensland State Archives.

Some of this information may be disclosed to: the offender's legal representatives, the Victims Register, other government Departments where statutory obligations exist (i.e. Commonwealth Department of Immigration and Ethnic Affairs and Attorney-General, law enforcement agencies and the courts), the Ombudsman, and Official Visitors.

Individuals can obtain information regarding access to their personal information by contacting the Manager, Information Rights Unit, email privacy@dcs.qld.gov.au or phone (07)323 93695.

The records are generally stored on paper and electronic media. The records may include videotape, audiotape and photographic image.

Location: Parole Board Secretariat, Level 3 Gabba Towers, 411 Vulture Street, Woolloongabba, 4102.

Intelligence and Investigation Records

The purpose of the Queensland Corrective Services Intelligence Group (QCSIG) is to collect, collate, analyse and disseminate intelligence relevant to the operations of the Agency. The intelligence may be used to manage risk (i.e. prisoner escapes, threats to offenders and staff) and manage security (e.g. security of facilities).

The Corrective Services Investigation Unit (CSIU) is a specialist branch of the Queensland Police Service and manages the investigation of, and where appropriate, prosecution of criminal matters within corrective facilities and offenders unlawfully at large from a facility.

The information may be obtained from a variety of sources and records primarily include information relating to criminal history and behaviour of offenders. Those who associate with or come into contact with offenders may also be subject to scrutiny if necessary.

Content may include: name, address, date of birth, gender, occupation, the offence and litigation process, physical description, education and criminal history.

Sensitive content may include details of: physical and mental health, racial or ethnic origin, criminal history, criminal intelligence, tax file numbers, financial information, relationships and families and associates of the offender.

The following Agency staff have access to the personal information subject to security authorisation and operational need: staff within QCSIG, senior management, Legal Services Branch and CSIU staff (records created by CSIU are accessed only by CSIU staff within the Agency) and authorised IT systems administration staff.

The records are kept in accordance with both the Agency's and the general retention and disposal schedules authorised by Queensland State Archives.

Some of the information may be disclosed to: law enforcement agencies (International, Commonwealth, State and Territory), the Public Trustee, legal counsel and the courts.

Individuals can obtain information regarding access to their personal information by contacting the Manager, Information Rights Unit, email privacy@dcs.qld.gov.au or phone (07)323 93695.

The records are generally stored on paper and electronic media. The records may include videotape, audiotape and photographic image.

Right to Information, Privacy, Judicial Review and Litigation Records

The purpose of these records is to process requests under the *Right to Information Act 2009* and the *Judicial Review Act 1991*, as well as for managing legal advice, litigation and coronial inquest matters. The personal information contained within these records may relate to the applicant, complainant, litigant or their representative and/or third parties to whom the application, complaint, litigation or coronial inquest relates.

Content may include: name, address, date of birth, gender, occupation, marital status, names and status of partners or relatives, information relating to offenders, victims, staff and other details relating to the particular request, complaint, litigation or coronial matter.

Sensitive content may include: physical and mental health, disabilities, racial or ethnic origin, religious or political affiliation, relationship details, criminal history, financial information, employment related information and offender management information.

The following Agency staff have access to some of this personal information subject to appropriate security authorisation and operational need: Legal Services Unit staff responding to Right to Information and Information Privacy requests, privacy complaints, applications for Judicial Review, requests for legal advice and litigation matters, staff in the functional areas of Agency responsible for providing the information or advice and senior management.

The records are kept in accordance with the general retention and disposal schedule issued by Queensland State Archives.

Some of the information may be disclosed to: Crown Law, the Queensland Police Service and other law enforcement agencies, counsel representing the Agency or the plaintiff, the courts, the Information Commissioner and the Ombudsman.

Individuals can obtain information regarding access to their personal information by contacting the Manager, Information Rights Unit, email privacy@dcs.qld.gov.au or phone (07)323 93695.

Legal advice and litigation records will usually be subject to legal privilege.

The records created by Legal Services officers are stored on paper and electronic media. The records accessed by officers may be paper based or electronic and may include photographic image, videotape and audiotape.

Location: Legal Services Unit, Emergency Services Complex, Park Road, Kedron 4031.

Victims Register

The Victims Register was established in 1997 and was formerly known as the Concerned Persons Register. It provides an information service for victims of crime and their families. The register enables the Agency to provide timely and accurate information to victims of crime regarding the offender who committed the offence/s against them.

Content about the offender may include: current location, the prisoner's classification, any transfers between corrective services facilities, eligibility dates for discharge or release, date of discharge or release. Content about the concerned person/s may include: their name and address and details of the offence.

Sensitive content about the offender may include: results of the prisoner's applications for parole orders, and other exceptional events relating to the prisoner such as death or escape from custody. Sensitive content about the concerned person/s may include: the name of the victim (if different from the Register applicant) and details about the offence.

The following agency staff have access to the personal information subject to security authority and operational need: Senior Adviser, Liaison Officer and Administration Office of the Victims Register and authorised IT system administration staff.

The records are kept in accordance with the Agency's retention and disposal schedule issued by Queensland State Archives.

The information is not normally disclosed to third parties other than the registered concerned person or an agency or person nominated by the concerned person and subject to approval by the chief executive or delegate of the Agency. Details concerning the concerned person's identity are not released outside the Agency.

Individuals can obtain information regarding access to their personal information by contacting the Manager, Information Rights Unit, email privacy@dcs.qld.gov.au or phone (07)323 93695.

The records are stored on paper and electronic media.

Location: Offender Programs and Services, 50 Ann Street, Brisbane 4000 or phone toll free 1800 098 098.

Official Visitor Records

Official visitors are appointed by the Director-General under the *Corrective Services Act 2006* to act as independent investigators of issues of concern raised by prisoners. On request, Official Visitors may review special treatment orders and maximum security orders. The purpose of the records is to report on individual investigations and provide summaries of complaints. A Register of Official Visitors is also maintained. All records are held securely in the Office of the Commissioner, Corrective Services.

Content may include: an Official Visitor's name, address and telephone number, and prisoner details including name, identification number and location.

Sensitive content may include: details from a prisoner's professional management, detention and health and medical files, investigation of the complaint, the official visitor report and recommendations.

The following Agency staff have access to this personal information if the prisoner has approved his/her identity being included in the report and wishes the Agency to respond to matters of concern that have been raised: general, managers of Correctional Centres, Chief Inspector and relevant administrative staff.

The records are kept in accordance with the standard retention and disposal schedule issued by Queensland State Archives.

Some of this information may be disclosed to the prisoner about whom the investigation relates and to other official visitors and investigative agencies. The Official Visitor has access to any Agency document relevant to the complaint being investigated.

Individuals can obtain information regarding access to their personal information by contacting the Manager, Information Rights Unit, email privacy@dcs.qld.gov.au or phone (07)323 93695.

The records are stored on paper and electronic media.

Location: Office of the Chief Inspector, 50 Ann Street, Brisbane 4001.

Ambulance Records

The Administrative Access Scheme provides a facility whereby patients can obtain access to and copies of their own patient treatment records, the service is provided on a fee basis. All other patient treatment records are managed in a confidential manner in compliance with Section 50 of the *Ambulance Service Act 1991*.

Location: Information Support Unit, Queensland Ambulance Service, Emergency Services Complex, Park Road, Kedron, phone (07) 310 97287.

Public registers managed within the Department

Public registers will be identified from time to time and their maintenance and use incorporated within the Department's personal information management practices.

Access and amendment procedures

Under the *Information Privacy Act 2009*, there are controls on how personal information is managed. The rights of access and amendment are dealt with in Information Privacy Principles (IPP) 6 and 7. Those rights are confined to the person to whom the personal information directly and personally relates.

IPP 6 provides that a person is entitled to access any record that contains their personal information except where access is restricted by any law.

IPP 7 provides that a person is entitled to seek an amendment of any record that contains their personal information that is misleading, irrelevant, not up-to-date or incomplete.

Applications for access to records containing personal information must be made in writing to the Department, as required by the *Information Privacy Act 2009*, and set out in detail the information to which access is requested.

Requests for access to, or amendment of, personal information must be dealt with through existing Right to Information and Information Privacy processes and should be forwarded to the Manager, Information Rights Unit, email privacy@dcs.qld.gov.au or phone (07)323 93695.

Complaint and Review Process

If an individual believes that the Department has not dealt with their personal information in accordance with the Information Privacy Principles (IPPs) within the *Information Privacy Act 2009*, they may make a complaint to the Department.

The Department must respond to complaints within 45 business days of receipt. If the complainant has lodged a formal written complaint and does not agree with the response they may refer a written complaint to the Office of the Information Commissioner.

Complaints or enquiries should be directed to the Manager, Information Rights Unit, GPO Box 1054, Brisbane, Qld 4001, email privacy@dcs.qld.gov.au or phone (07)323 93695.

If you would like complaint handling documents sent to you, more information on the complaints process or on privacy matters in general, please contact the Manager, Information Rights Unit, email privacy@dcs.qld.gov.au or phone (07)323 93695.

Acts administered by the Department of Community Safety

[Corrective Services Act 2006](#)

[Corrective Services Regulation 2006](#)

[Parole Orders \(Transfer\) Act 1984](#)

[Ambulance Service Act 1991](#)

[Ambulance Service Regulation 2003](#)

[Fire and Rescue Service Act 1990](#)

[Fire and Rescue Service Amendment Regulation \(No.1\) 2009](#)

[Disaster Management Act 2003](#)

[Building Fire Safety Regulation 2008](#)

The following legislation, not administered by the Agency, is very relevant to its activities:

[Acts Interpretation Act 1954](#)

[Anti-Discrimination Act 1991](#)

[Bail Act 1980](#)
[Commission for Children and Young People and Child Guardian Act 2000](#)
[Coroners Act 2003](#)
[Crimes Act 1914](#)
[Criminal Code Act 1899](#)
[Criminal Law \(Rehabilitation of Offenders\) Act 1986](#)
[Criminal Law Amendment Act 1945](#)
[Criminal Offence Victims Act 1995](#)
[Drugs Misuse Act 1986](#)
[Drug Court Act 2000](#)
[Evidence Act 1977](#)
[Financial Administration and Audit Act 1977](#)
[Financial Management Standard 1997](#)
[Information Privacy Act 2009](#)
[Judicial Review Act 1991](#)
[Justices Act 1886](#)
[Juvenile Justice Act 1992](#)
[Juvenile Justice REGULATION 2003](#)
[Legislative Standards Act 1992](#)
[Mental Health Act 2000](#)
[Penalties and Sentences Act 1992](#)
[Personal Injuries Proceedings Act 2002](#)
[Prisoners \(Interstate Transfer\) Act 1982](#)
[Prisoners International Transfer \(Queensland\) Act 1997](#)
[Public Records Act 2002](#)
[Public Sector Ethics Act 1994](#)
[Public Service Act 2008](#)
[Public Trustee Act 1978](#)
[Recording of Evidence Act 1962](#)
[Right to Information Act 2009](#)
[Social Security \(Administration\) Act 1999 \(Clth\)](#)
[State Penalties Enforcement Act 1999](#)
[Statutory Instruments Act 1992](#)
[Trust Accounts Act 1973](#)
[Trust Accounts Regulation 1999](#)
[Uniform Civil Procedure Rules 1999](#)
[Veterans Entitlement Act 1986 \(Clth\)](#)
[Weapons Act 1990](#)
[Whistleblower Protection Act 1994](#)
[Witness Protection Act 2000](#)
[Workers Compensation and Rehabilitation Act 2003](#)
[Workplace Health and Safety Act 1995](#)
[Young Offenders \(Interstate Transfer\) Act 1987](#)

Appendix 1

Information Privacy Principles (IPPs)

Information Privacy Principle 1

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

- (a) the information is collected for a lawful purpose directly related to a function or activity of the agency; and
- (b) the collection of the information is necessary to fulfil the purpose or is directly related to fulfilling the purpose.

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

Information Privacy Principle 2

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

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

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

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

- (a) the purpose of the collection; and
- (b) if the collection of the personal information is authorised or required under a law—
 - (i) the fact that the collection of the information is authorised or required under a law; and
 - (ii) the law authorising or requiring the collection; and
- (c) if it is the agency's usual practice to disclose personal information of the type collected to any entity (the first entity)—the identity of the first entity; and
- (d) if the agency is aware that it is the usual practice of the first entity to pass on information of the type collected to another entity (the second entity)—the identity of the second entity.

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

- (a) if practicable—before the personal information is collected; or
- (b) otherwise—as soon as practicable after the personal information is collected.

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

- (a) the personal information is collected in the context of the delivery of an emergency service; and Example— personal information collected during a triple 0 emergency call or during the giving of treatment or assistance to a person in need of an emergency service
- (b) the agency reasonably believes there would be little practical benefit to the individual in complying with subsection (3) in the circumstances; and
- (c) the individual would not reasonably expect to be made aware of the matters mentioned in subsection (3).

Information Privacy Principle 3

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

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

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

- (a) the personal information collected is—
 - (i) relevant to the purpose for which it is collected; and
 - (ii) complete and up to date; and
- (b) the extent to which personal information is collected from the individual the subject of it, and the way personal information is collected, are not an unreasonable intrusion into the personal affairs of the individual.

Information Privacy Principle 4

- (1) An agency having control of a document containing personal information must ensure that—
 - (a) the document is protected against—
 - (i) loss; and
 - (ii) unauthorised access, use, modification or disclosure; and
 - (iii) any other misuse; and
 - (b) if it is necessary for the document to be given to a person in connection with the provision of a service to the agency, the agency takes all reasonable steps to prevent unauthorised use or disclosure of the personal information by the person.
- (2) Protection under subsection (1) must include the security safeguards adequate to provide the level of protection that can reasonably be expected to be provided.

Information Privacy Principle 5

- (1) An agency having control of documents containing personal information must take all reasonable steps to ensure that a person can find out—
 - (a) whether the agency has control of any documents containing personal information; and
 - (b) the type of personal information contained in the documents; and
 - (c) the main purposes for which personal information included in the documents is used; and
 - (d) what an individual should do to obtain access to a document containing personal information about the individual.
- (2) An agency is not required to give a person information under subsection (1) if, under an access law, the agency is authorised or required to refuse to give that information to the person.

Information Privacy Principle 6

- (1) An agency having control of a document containing personal information must give an individual the subject of the personal information access to the document if the individual asks for access.
- (2) An agency is not required to give an individual access to a document under subsection (1) if—
 - (a) the agency is authorised or required under an access law to refuse to give the access to the individual; or
 - (b) the document is expressly excluded from the operation of an access law.

Information Privacy Principle 7

- (1) An agency having control of a document containing personal information must take all reasonable steps, including by the making of an appropriate amendment, to ensure the personal information—
 - (a) is accurate; and
 - (b) having regard to the purpose for which it was collectedor is to be used and to any purpose directly related to fulfilling the purpose, is relevant, complete, up to date and not misleading.
- (2) Subsection (1) applies subject to any limitation in a law of the State providing for the amendment of personal information held by the agency.
- (3) Subsection (4) applies if—
 - (a) an agency considers it is not required to amend personal information included in a document under the agency's in a way asked for by the individual the subject of the personal information; and
 - (b) no decision or recommendation to the effect that the document should be amended wholly or partly in the way asked for has been made under a law mentioned in subsection (2).
- (4) The agency must, if the individual asks, take all reasonable steps to attach to the document any statement provided by the individual of the amendment asked for.

Information Privacy Principle 8

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

Information Privacy Principle 9

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

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

Information Privacy Principle 10

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

- (a) the individual the subject of the personal information has expressly or impliedly agreed to the use of the information for the other purpose; or
- (b) the agency is satisfied on reasonable grounds that use of the information for the other purpose is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare; or
- (c) use of the information for the other purpose is authorised or required under a law; or
- (d) the agency is satisfied on reasonable grounds that use of the information for the other purpose is necessary for 1 or more of the following by or for a law enforcement agency—
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties or sanctions;
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
 - (iii) the protection of the public revenue;
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct;
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or
- (e) the other purpose is directly related to the purpose for which the information was obtained; or

Examples for paragraph (e)—

- 1 An agency collects personal information for staff administration purposes. A new system of staff administration is introduced into the agency, with much greater functionality. Under this paragraph, it would be appropriate to transfer the personal information into the new system.
- 2 An agency uses personal information, obtained for the purposes of operating core services, for the purposes of planning and delivering improvements to the core services.

(f) all of the following apply—

- (i) the use is necessary for research, or the compilation or analysis of statistics, in the public interest;
- (ii) the use does not involve the publication of all or any of the personal information in a form that identifies any particular individual the subject of the personal information;
- (iii) it is not practicable to obtain the express or implied agreement of each individual the subject of the personal information before the use.

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

Information Privacy Principle 11

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

- (a) the individual is reasonably likely to have been aware, or to have been made aware, under IPP 2 or under a policy or other arrangement in operation before the commencement of this schedule, that it is the agency's usual practice to disclose that type of personal information to the relevant entity; or
- (b) the individual has expressly or impliedly agreed to the disclosure; or
- (c) the agency is satisfied on reasonable grounds that the disclosure is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare; or

- (d) the disclosure is authorised or required under a law; or
- (e) the agency is satisfied on reasonable grounds that the disclosure of the information is necessary for 1 or more of the following by or for a law enforcement agency—
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties or sanctions;
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
 - (iii) the protection of the public revenue;
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct;
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or
- (f) all of the following apply—
 - (i) the disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest;
 - (ii) the disclosure does not involve the publication of all or any of the personal information in a form that identifies the individual;
 - (iii) it is not practicable to obtain the express or implied agreement of the individual before the disclosure;
 - (iv) the agency is satisfied on reasonable grounds that the relevant entity will not disclose the personal information to another entity.

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

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

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

- (a) it is impracticable for the relevant entity to seek the consent of the individual before the personal information is used for the purposes of the marketing; and
- (b) the relevant entity will not charge the individual for giving effect to a request from the individual to the entity that the individual not receive any marketing communications; and
- (c) the individual has not made a request mentioned in paragraph (b); and
- (d) in each marketing communication with the individual, the relevant entity will draw to the individual's attention, or prominently display a notice, that the individual may ask not to receive any further marketing communications; and
- (e) each written marketing communication from the relevant entity to the individual, up to and including the communication that involves the use, will state the relevant entity's business address and telephone number and, if the communication with the individual is made by fax, or other electronic means, a number or address at which the relevant entity can be directly contacted electronically.