Department of Families, Seniors,
Disability Services and Child Safety

Information Privacy Policy

Department of Families, Seniors, Disability Services & Child Safety

July 2025

Queensland Government

Contents

The *Information Privacy Act 2009* (Qld) (IP Act) regulates how public sector agencies such as the Department of Families, Seniors, Disability Services and Child Safety (the department) collect, manage, use and disclose personal information.

This Privacy Policy is prepared in compliance with the department's obligation under Queensland Privacy Principle (QPP) 1.3. It contains information about:

- the kinds of personal information that the department collects and holds
- how the department collects and holds personal information
- the purposes for which the department collects, holds, uses and discloses personal information
- how you can access information the department holds about you and how you can seek correction of the information
- how you can make a complaint about a possible breach of the department's obligations under the IP Act, and how the department will deal with the complaint
- whether the department discloses personal information to entities outside Australia.

1. Obligations under the IP Act

The IP Act:

- creates an obligation on the department to comply with the QPPs
- regulates when personal information may be disclosed outside of Australia, and
- outlines the department's obligations regarding contracted service providers.

1.1 What is personal information?

Personal information is defined in section 12 of the IP Act as:

> *information or an opinion about an identifiable individual or an individual who is reasonably identifiable, from the information or opinion –*
> *(a) whether the information or opinion is true or not; and*
> *(b) whether the information or opinion is recorded in a material form or not.*

Personal information may be stored in many formats, including hard copy (e.g. paper, photograph, video/audiotape) or electronic (e.g. in an electronic database or digital format).

An individual will be *identified* where they can be identified from the information itself, without referring to any other information. They will be reasonably identifiable if there is reasonable potential that multiple pieces of information could lead to their identity being known.

The likelihood of an individual being reasonably identifiable may depend on multiple factors relevant to the information, the characteristics of the individual, and the agency's functions.

Some personal information is *sensitive information.* Sensitive information includes:

- information or opinion about an individual's:
  - racial or ethnic origin
  - political opinions
  - membership of a political association
  - religious beliefs or affiliations
  - philosophical beliefs
  - membership of a professional or trade association

  - membership of a trade union
  - sexual orientation or practices, or
  - criminal record; or
- health information
- genetic information
- biometric information and biometric templates.

There are additional obligations in relation to the collection, use and disclosure of sensitive information.

1.2 What are the QPPs?

The ten QPPs set out how personal information must be managed, including:

QPP 1: Open and transparent management of personal information
QPP 2: Anonymity and pseudonymity
QPP 3: Collection of solicited personal information
QPP 4: Dealing with unsolicited personal information
QPP 5: Notification of the collection of personal information
QPP 6: Use or disclosure of personal information
QPP 10: Quality of personal information
QPP 11: Security of personal information
QPP12: Access to personal information
QPP13: Correction of personal information [1]

1.3 Contracted service providers

Where the department enters into a contract or other arrangement for the provision of services that deal with personal information, the department must take all reasonable steps to bind the service provider to comply with the IP Act. If it does not do so, the department may be liable for any privacy breaches by the service provider.

1.4 Disclosing personal information overseas

The IP Act also regulates the disclosure of personal information to entities outside Australia. This may be relevant if personal information is stored on computer networks and servers outside Australia and accessible by the service provider (e.g. some cloud-based service providers are located overseas).

Under the IP Act, the department may disclose personal information outside Australia only if it complies with the various requirements set out in section 33 of the IP Act, including:

- the person has agreed to the disclosure, or
- the disclosure is authorised or required by law, or
- there are reasonable grounds to believe the disclosure is necessary to prevent or lessen a serious threat to someone's life, health, safety, or welfare, or public health, safety or welfare, or

[1] **Note:** The QPPs have been drafted to align with the federal Australian Privacy Principles (APPs), but as there are some APPs which are not relevant to State Government agencies, the QPP numbers are not consecutive.

- the department is satisfied that the information will be subject to privacy protections that are substantially similar to the QPPs and has taken reasonable steps to ensure that the information will not be treated in a way inconsistent with the QPPs.

Generally, the department does not transfer personal information outside Australia. Any proposal to store personal information stored offshore needs to comply with the *Information Privacy Act 2009*. In addition, other, statutory, or legal requirements may apply depending on the specific data and/or information.

1.5 Documents to which privacy principles do not apply.

The privacy principles do not apply to certain documents such as:

- generally available publications
- documents held in a library, art gallery or museum for reference, study or exhibition
- public records under the *Public Records Act 2002* in the custody of Queensland State Archives that are not in a restricted access period under that Act
- a letter, or anything else, while it is being transmitted by post
- a document to the extent it contains personal information—
  - relating to a controlled operation or activity under the *Police Powers and Responsibilities Act 2000* or the *Crime and Corruption Act 2001*
  - relating to covert operations, investigations or law enforcement agency functions
  - obtained under a warrant issued under the *Telecommunications (Interception and Access) Act 1979* (Cwlth)
  - witness protection information
  - relating to complaints under the *Police Service Administration Act 1990*
  - relating to complaints and investigations of corruption under the *Crime and Corruption Act 2001*
  - public interest disclosures under the *Public Interest Disclosure Act 2010*
  - Cabinet and Executive Council information which would be exempt under the *Right to Information Act 2009* (RTI Act)
  - documents arising out of a commission of inquiry.

2. About the department

The department collects, holds, uses, and discloses personal information in order to perform its functions. The main business areas that collect personal information for the purposes of their service delivery, regulatory, legislative, and administrative activities are:

- Adoption
- Child and Family Services (including Delegated Authority and Office of the Child and Family Official Solicitor)
- Community Recovery
- Disability Services
- Families and Communities
- National Redress Scheme
- Prevention of domestic and family violence
- Seniors and carers, and

- Corporate Services.

The department administers (or jointly administers) legislation relating to the delivery of these services and may deal with personal information when doing so. Key legislation includes:

- *Adoption Act 2009*
- *Carers (Recognition) Act 2008*
- *Child Protection Act 1999*
- *Child Protection (International Measures) Act 2003*
- *Child Safe Organisations Act 2024*
- *Community Services Act 2007*
- *Disability Services Act 2006*
- *Domestic and Family Violence Protection Act 2012*
- *Forensic Disability Act 2011*
- *Guide, Hearing and Assistance Dogs Act 2009*
- *National Disability Insurance Scheme Act 2013* (Cwth)
- NDIS (Restrictive Practices and Behaviour Support) Rules 2018 (Cwth)
- *Privacy Act 1988* (Cwth)
- *National Redress Scheme for Institutional Child Sexual Abuse Act 2018* (Cwth)
- *National Redress Scheme for Institutional Child Sexual Abuse (Commonwealth Powers) Act 2018*

In addition, Corporate Services provides support services including human resources, staff support, finance, procurement, legal advice, audits and compliance, information access and Redress (to acknowledge and support people who experienced sexual abuse in an institutional setting). Key legislation includes:

- *Anti-Discrimination Act 1991*
- *Crime and Corruption Act 2001*
- *Financial Accountability Act 2009*
- *Financial and Performance Management Standard 2009*
- *Human Rights Act 2019*
- *Information Privacy Act 2009*
- *National Redress Scheme for Institutional Child Sexual Abuse (Commonwealth Powers) Act 2018*
- *National Redress Scheme for Institutional Child Sexual Abuse Act 2018* (Cth)
- *Public Records Act 2002*
- *Public Sector Act 2022*
- *Public Sector Ethics Act 1994*
- *Right to Information Act 2009*
- *Work Health and Safety Act 2011*
- *Workers' Compensation and Rehabilitation Act 2003*

More details about the functions and services provided by the above areas of the department are found in **Appendix 1** of this policy.

3. Collection of personal information

3.1 What personal information do we collect and hold?

The department only collects the information it needs to carry out its functions and activities, including regulatory, legislative, and administrative activities.

This may include information about:

- clients, family members and carers
- support persons and authorised representatives
- departmental employees, including prospective employees, and contractors
- representatives and employees of non-government service providers
- representatives of organisations, local governments and members of ministerial advisory committees that may be constituted from time to time
- vendors and service providers.

The types of personal information collected will depend on the function or activity staff are performing, but may include:

- name and contact details
- date of birth
- signature
- photograph
- financial/bank details, including Centrelink and Veteran Affairs information
- unique identifying numbers (e.g. tax file number, driver licence number)
- cultural background
- family and relationship details
- child protection history and allegations of harm
- medical/health/diagnostic information
- educational needs and service provision needs
- adoption information
- occupation and employment history
- details of office bearers in funded organisations
- offending and criminal history
- details about persons making complaints, subjects of complaints and witnesses
- recruitment information, such as applications, curriculum vitae, referee reports, interview notes and selection panel assessments
- information about staff relevant to human resource management functions (e.g. leave entitlements, bank account details, superannuation information, pay scale)
- footage captured by camera surveillance systems or electronic monitoring devices in departmental premises, such as service centre counters.

As far as possible, we collect this information directly from you. However, it may also be necessary to collect information from third parties e.g. other family members, carers, health service providers, educators (childcare and school-based), and Queensland Police Services. Sometimes people will contact the department and share information about you.

Generally, the department will tell you when this has happened. Sometimes we may not be able to tell you for some time, e.g. if an investigation is under way and discussing the information with you may prejudice the investigation. We may not be able to tell you at all, if doing so could disclose the identity of a confidential source of information.

3.2 Sensitive information

Some of this information is *sensitive information*. The department may need to collect sensitive information about you, for example:

- to respond to an allegation of harm in relation to a child
- to provide disability services to you
- to handle a complaint, or
- for recruitment processes if you apply for a job with the department.

Specific obligations apply to the collection, use and disclosure of sensitive information.

3.3 Anonymity & pseudonymity

As far as reasonably possible, you have the option to interact with the department anonymously or using a pseudonym.

For example: if you contact the department to make a notification or a complaint, you may do so anonymously.

However, for most interactions with the department, your name and contact information will be required to enable the department to deal with the matter fairly and efficiently.

For example: it is not possible to complete a carer assessment without knowing your identity, because it is necessary to conduct checks to assess your suitability, including domestic and family violence, traffic history and criminal history checks. These cannot be done without the department confirming your identity. However, these checks are only done with your consent.

If you do choose to deal with the department anonymously, the department may not be able to provide feedback about the matters you raise with us or seek additional information which may be necessary in order to take effective action in relation to the information you provide.

3.4 How do we collect and hold personal information?

3.4.1 Direct collection

When we collect personal information from you, we take reasonable steps to explain to you:

- why your information is being collected
- when the department might collect personal information from third parties
- whether the collection is required or authorised under an Australian law, or a court or tribunal order
- the purpose of the collection
- the main consequences if all or some of the personal information is not collected
- any other agency or entity to whom the department usually discloses personal information of this type
- whether your information might be disclosed to an entity outside Australia and if so, the countries in which the recipients are likely to be located
- the department's privacy policy includes information about how to access and correct your personal information, how to make a privacy complaint and how it will be dealt with.

This information may be given verbally or in writing (e.g. on a form, a pamphlet, or a sign).

3.4.2 Indirect collection

We may also collect personal information about you, including sensitive information, indirectly, from publicly available sources, or from third parties such as:

- your authorised representative, if you have one
- friends, family, neighbours
- professionals you have been involved with (e.g. medical or educational professionals)
- other government agencies (including State and Territory child protection or disability services bodies, schools, hospitals, police) who may be aware of information about you which is relevant to the performance of the department's functions.

For example: we may collect information about you from third parties if:

- the department has been notified about concerns relating to your child, and it is assessed that family members, support persons, neighbours, teachers or medical professionals who are working with your family may have relevant information; or

- you are receiving disability services from Accommodation Support and Respite Services (AS&RS), and your authorised representative has information about your needs.

3.4.3 Methods of collection

The department collects personal information by various methods, including face-to-face meetings, telephone calls, hard copy forms, web-based forms, emails, submissions, and surveys. Some of these methods of collection are discussed below.

Email

Emails which contain information the department is required to retain as public records will be captured into the department's recordkeeping systems.

However, the department will not add your name and address details to a mailing list or disclose these details to third parties without your consent, unless required by law.

Smart Service Queensland

The department uses Smart Service Queensland to enable you to, for example, lodge a complaint, enquiry or apply for a job. The department collects personal information that you provide through the use of Smart Service Queensland.

Further information about the Smart Service Queensland can be found here.

Camera surveillance systems

The department uses camera surveillance systems in some locations, including at Child Safety Service Centres (CSSCs), communal areas of AS&RS and office locations. Generally, this is done for safety and security reasons. There will be signs advising you if camera surveillance is in use.

Footage is only retained for a short period (e.g. 30 days). After that time, it is overwritten and cannot be retrieved. Footage can be extracted and copied if, for example, there is an incident and the footage is assessed to be relevant, or an access request is received.

Therefore, if you wish to obtain a copy of footage which includes your image, you should notify the department's Information Access and Amendment Team as soon as possible. It is usually necessary to make a formal application under *Right to Information Act 2009* for camera surveillance footage. The process for applying for information is discussed below.

Web analytics and cookies

When you visit the department's website, our web measurement tool and internet service provider records anonymous information for statistical purposes, including:

- the type of browser, computer platform and screen resolution you are using
- your traffic patterns through our site, such as:
    - pages you accessed and documents downloaded
    - the page you visited prior to accessing our site
    - the IP address of the server accessing our site.

Our web measurement software uses cookies to collect this information. Cookies are small data files transferred onto computers or devices by websites for record-keeping purposes and to enhance functionality on the website. Most browsers allow you to choose whether to accept cookies or not. If you do not wish to have cookies placed on your computer, please set your browser preferences to reject all cookies before accessing our website.

If it is collected, the department does not attempt to identify you from this information, or to use or disclose identifying information, unless required by law.

Social networking services

The department uses social networking services such as Twitter, Facebook and LinkedIn to communicate with the public about our work. When you communicate with us using these services we may collect your personal information, but we only use it to help us to communicate with you and the public.

Social networking services will also handle your personal information for their own purposes. These services have their own privacy policies. For example, you can access the privacy policies for Twitter, Facebook and LinkedIn on their websites.

Surveys

The department may use tools such as Survey Monkey to conduct surveys. Generally, the department does not seek to collect personal information in your survey responses. However, information which is collected by Survey Monkey and other tools may be stored overseas. You will be advised if that will occur and that by proceeding you will be taken to consent to the overseas transfer of any personal information you provide.

Survey Monkey's privacy statement is available here.

Mailing lists and event registrations

The department collects personal information such as contact details that you provide when signing up to mailing lists, registering for events, or when submitting feedback about your experience with the department's website.

Information about you is also collected by the department when you open, click on links or download any image in an email sent to you via a departmental mailing list. The information collected includes:

- whether you opened an email sent to you via a departmental mailing list
- which links you click in those emails
- your mail client (e.g. 'Outlook' or 'iPhone')
- if interactions with those emails occurred on a mobile or desktop environment, and
- the country geolocation of your IP address (the IP address itself is not stored).

The department uses Vision6 to manage its mailing lists and event registrations. Vision6's privacy policy is available here.

3.4.4 Quality of personal information

To ensure that the personal information we collect is accurate, up-to-date and complete we:

- promptly capture information (including updated information) into record-keeping systems in a consistent format
- where appropriate, confirm the accuracy of information we collect from a third party or another source, and
- where appropriate, check that personal information is still accurate and current before using or disclosing it.

4. Use and disclosure of personal information

4.1 Purposes for which we use/disclose your information

Generally, the department only uses and discloses your personal information for the purpose for which it was collected (primary purpose). However, the department may use or disclose your personal information for a different purpose (secondary purpose) if one of the exceptions in QPP 6 applies. For example, if:

- you consent
- you would reasonably expect the department to use or disclose the information for the secondary purpose and:
  - if it is sensitive information, the secondary purpose is directly related to the primary purpose
  - if it is not sensitive information, the secondary purpose is related to the primary purpose
- the use or disclosure is authorised or required under an Australian law or a court or tribunal order, e.g. in response to a subpoena relating to legal proceedings
- a permitted general situation exists, including:
  - it is unreasonable or impractical to obtain your consent and the department reasonably believes that it is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or the public
  - the department suspects that there is unlawful activity or serious misconduct relating to its functions or activities and reasonably believes that the collection, use or disclosure is necessary so it can take appropriate action
  - the department reasonably believes that it is reasonably necessary to assist an entity to locate a person who has been reported missing, and the collection, use or disclosure complies with a guideline under chapter 3, part 2, IP Act
  - it is reasonably necessary to establish, exercise or defend a legal or equitable claim
  - it is reasonably necessary for a confidential alternative dispute resolution process

- the department reasonably believes the use or disclosure is reasonably necessary for enforcement-related activities conducted by a law enforcement agency, or
- the use or disclosure is for research in the public interest.

4.2 Primary purpose uses

The department uses personal information for the purpose for which it was collected, e.g.:

- exercise its powers or perform its functions and duties
- carry out analytics, business improvement and reporting, and
- process job applications.

4.2.1 Powers, functions and duties of the department

Some examples of where the department may use your personal information for the purpose of exercising its powers or performing its functions or duties include:

- using your contact details to respond to you about an enquiry or RTI application
- using information, you provide in a complaint to ascertain what occurred
- monitoring email traffic for trouble shooting or maintenance purposes
- generating reports from data in the department's Data Warehouse for business intelligence functions, including the creation of internal and external reports
- internal alerts to staff phones and email e.g. about office closures, ICT outages, office evacuations, and health and safety concerns.

4.2.2 Document Verification Services

If you consent, the department may use a government identity verification service.

Some departmental services may use the Commonwealth Document Verification Service (DVS) (also known as IDMatch) through the Attorney-General's Department (AGD) user interface to electronically verify proof of identity (POI) documents, such as a birth certificates or passports which you provide. Using DVS means that the department does not need to obtain or keep copies of your identity documents. The AGD will not retain any documents provided to it once the verification process is complete; transaction data is retained for the minimum period required under law and for auditing purposes.

Other departmental services may use the Queensland Digital Identity (QDI) system. QDI is a modern, robust an innovative system which meets the highest national standards and security protocols for digital identity; for example, QDI is used in the Digital Licence App. You should never share your login details with anyone. If someone attempts to use your QDI they would need to know your email address, your password, and have possession of your mobile phone. Like with the DVS, using QDI means that the department does not need to obtain or keep copies of your identity documents. Once a QDI is verified, we take note of the credentials that were used, so that they cannot be used again to verify for a different QDI. More information is available at About the Queensland Digital Identity | Queensland Government.

The Disability Worker Screening Portal uses verification provided by the Department of Transport and Main Roads (TMR) when creating an account. Identity information is checked against the TMR web service and, if valid, the user is added to the system. When subsequently logging in, users enter their Licence Number and date of birth. This information is checked in the database (not TMR) and a 6-digit verification is emailed to them, which must be entered to complete the log-in process. As above, the use of this process means that the department does not need to collect or keep copies of your identity documents. More information is available in the Identity Verification Process for Workers fact sheet.

4.2.3 Job applications

The department collects personal information which you provide in support of a job application including your:

- name
- address
- contact details
- application and resume, and
- identification information (including in relation to citizenship/residence eligibility).

This personal information is used to assess your job application, including your eligibility to apply for the advertised position.

The department may also use third party services such as RefHub to obtain referee reports. You will be advised if this is going to occur. This may include Artificial Intelligence (AI) features such as evaluating candidate answers, fraud detection and generating executive summaries of referee reports. RefHub handles personal information in accordance with its privacy policy.

Human resources information

In addition to job applications, the department collects and uses personal information of its employees for human resources purposes, including:

- pay, superannuation and tax information
- evidence of identity and eligibility (e.g. residence/citizenship) information
- criminal history and blue card information
- diversity information including, age, sexual orientation, ethnicity (usually optional)
- next of kin details
- leave history, including medical certificates
- training and development information
- information about staff performance, including allegations of misconduct and corrupt conduct.

Queensland Shared Services (QSS) is a shared service provider delivering finance, procurement, human resources and telecommunication support and systems. The department uses QSS to provide these services. The department has entered into a Service Level Agreement with QSS in relation to the provision of these services, to ensure it maintains control of and secures human resources information it received under this arrangement.

4.2.4 Analytics, business improvement and reporting

The department uses information collected using its various analytics tools and survey platforms, for business improvement processes, for example, information about your interactions with the department website is used to improve your website user experience.

Generally, the department does not collect identifying information for this purpose. If identifying information is collected, it is de-identified before it is used for analytics, business improvement and reporting purposes.

4.3 Secondary purpose uses

In certain circumstances, the department may use your personal and sensitive information for a different purpose to that for which it was collected.

Generally, the department only uses your sensitive information with your consent. However, we may use your sensitive information for a secondary purpose without your consent, if:

- it is required or authorised by or under law, or
- a permitted general situation exists (e.g. if the department reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or the public and it is unreasonable or impracticable to obtain your consent).

4.4 Disclosures

The department may disclose personal information to external entities in certain circumstances, discussed below.

4.4.1 External reporting

The department is required by law to produce certain external reports, usually for government oversight of its activities.

The department may use your personal information to generate these reports, usually by way of the department's Data Platforms and use of business intelligence software. However, your personal information will be in the form of either aggregated data that does not identify you or information that will be de-identified before release of such reports.

4.4.2 Statutory information sharing

Under the IP Act the department may share your personal information where information sharing is authorised under relevant legislation.

For example:

- The department will provide documents containing personal information to the Director of Child Protection Litigation in child protection litigation matters. This information is shared in accordance with the *Director of Child Protection Litigation Act 2016.* Personal information of people who have been involved in the matter may be included in applications and affidavits provided to parties to the litigation, including parents, and to the Court.

- The department may provide personal information to other stakeholders, including government agencies (such as Queensland Police Service, Queensland Health, Education Queensland), in accordance with the *Child Protection Act 1999* (e.g. to ensure that safety and wellbeing of children, or to locate a missing person).

- The department may provide documents containing personal information to review and oversight bodies such as the Queensland Family and Child Commission, the Ombudsman, National Disability Insurance Scheme (NDIS) Quality and Safeguards Commission, the Queensland Health Ombudsman, the Information Commissioner, the Privacy Commissioner, the Queensland Human Rights Commission, under relevant legislation.

- The department provides information to the Together Queensland Industrial Union of Employees and the Australian Workers' Union of Employees, Queensland (e.g. new starter details including name, job title, work location and work email address); and a full staff listing (name, job title and work location) every six months, as required under the Union Encouragement paragraph of the Certified Agreement.

- The department provides allegations of corrupt conduct to the Crime and Corruption Commission, in accordance with the *Crime and Corruption Act 2001.* Allegations of misconduct by SES 3 and above are also reported to the Public Service Commission.

- The department provides information about suspected criminal activity to the Queensland Police Service for investigation and possible prosecution.

4.4.3 Complaints and reviews

If you make a complaint to the department, it may be necessary for us to disclose information you provide or other information about you to the alleged person responsible and others who may have information about what occurred. It is necessary to do this so that we can properly assess and respond to your complaint, and to provide procedural fairness to the person complained about.

The department may also disclose personal information to a review or oversight body as outlined above.

4.4.4 Information given for publication

If you publish your personal information or provide it to someone for the purpose of publication, the department is not required to comply with QPP 6 or QPP 10.2 in relation to that information and connected or related information. This means that the department may disclose additional information in response to the matters raised by you, e.g. by way of explanation about why the department took a particular action.

4.4.5 Data breach notifications

The department is required to notify relevant bodies about privacy breaches.

For example: If a privacy breach occurs in relation to the department's use of information in the My Health Records System, the *My Health Records Act 2012* (Cth) requires the department to notify the My Health Records System Operator. That notification may include your personal information if you are affected by the breach.

For example: The *Privacy Act 1988* (Cth) requires the department to notify the Office of the Australian Information Commissioner (OAIC) about a privacy breach affecting Tax File Numbers (TFNs). If employee TFNs are affected by a data breach, identifying employee information may be provided to the OAIC.

4.4.6 Disclosure of sensitive information

Generally, the department will only disclose your sensitive information with your consent.

However, there are some exceptions that permit disclosure of sensitive information for a secondary purpose without your consent, including:

- where it is required or authorised by or under law
- where it is unreasonable or impracticable to obtain your consent and the department reasonably believes that the disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual or the public
- the department suspects unlawful activity or serious misconduct and reasonably believes that the disclosure is necessary for it to take appropriate action
- the department reasonably believes that the disclosure is reasonably necessary to help locate a missing person, or
- the use or disclosure is reasonably necessary to establish, exercise or defend a legal or equitable claim, or for a confidential alternative dispute resolution process.

4.4.7 Disclosure of personal information overseas

The department only discloses personal information overseas in limited circumstances, for example, to respond to a complaint if the complainant or respondent is based overseas. Some analytical data collected by tools such as Google Analytics may be stored in cloud-based servers in the United States.

When you communicate with the department through a social network service such as Facebook or Twitter, the social network provider and its partners may collect and hold your personal information overseas.

5. Storage and security

5.1 General

Hard copy documents are either held on site, on secure floors and in a mixture of tambours and locked cabinets, or in secure offsite storage.

Personal information collected in an electronic format is held on servers located in Australia, either on-premise or in dedicated government tenancies in the cloud. The department retains effective control over all personal information held on the government cloud tenancy, and the information is handled in accordance with the QPPs.

5.2 Information technology security practices

The department takes reasonable steps to protect the personal information it holds from internal and external threats. For example, the department:

- applies mitigation strategies developed by the Australian Signals Directorate known as the 'Essential Eight', including multi-factor authentication, restricted administrative privileges, regular back-ups, promptly implementing updates and patches
- implements audit and scanning controls to detect unauthorised access to department systems and information (e.g. using another person's account; viewing, sharing or storing inappropriate material; and using unauthorised devices)
- keeps a record (audit trail) of when personal information held in the department's electronic databases is changed or deleted
- conducts regular internal and external audits
- has comprehensive information security policies and procedures, awareness campaigns and mandatory staff training
- regularly reviews and updates the department's Data Breach Response Plan to ensure that the department meets its obligations under the Mandatory Data Breach Notification Scheme under the IP Act, and
- undertakes Privacy Impact Assessments when information handling practices change, or new practices are introduced.

5.3 Destruction or deletion of personal information

Personal information which is contained in a departmental record is subject to the requirements of the *Public Records Act 2023*, the General Retention and Disposal Schedule, and any other applicable Retention and Disposal Schedule. Some records, for example adoption and child protection records, have indefinite or very long retention periods.

When it is authorised or required to dispose of documents, the department destroys personal information in a secure manner.

6. Access and correction

Under QPP 12, you have a right to ask for access to personal information the department holds about you. The department facilitates access to certain types of personal information through administrative access schemes, or you can make a formal application under the *Right to Information Act 2009* (RTI Act).

Under QPP 13, you have a right to ask the department to correct personal information we hold about you if you believe that the information is inaccurate, out of date, incomplete, irrelevant or misleading.

These processes are discussed below.

6.1 Administrative access

The department has administrative access schemes which you may be able to use to access your personal information instead of making an application under the IP Act or RTI Act. Information about those schemes is available on the department's website.

When you ask for your personal information, we require evidence of your identity to ensure that your personal information is not disclosed inappropriately.

Sometimes administrative access will not be appropriate, for example, if information about other people is recorded with your information. In those cases, a formal application under the RTI Act is usually required because the documents must be redacted to remove third party information.

6.2 Formal applications for access

There are no application fees or charges for access to your own personal information under the RTI Act. However, if you want information about someone else, or information which is not your personal information, an application fee will apply. There may also be processing and access charges.

For an application for access to be valid it **must**:

- contain the information listed in the RTI Act
- give enough information about the document/s you are seeking to enable the documents to be identified
- be accompanied by evidence of your identity, and
- provide an address to which notices under the RTI Act can be sent.

There is information about how to apply, including a link to a online application form available at About Right to Information and Information Privacy applications.

If you are seeking access to your personal information, you must provide evidence of your identity, to ensure that your information is not disclosed to anyone else. Include certified copies of identification documents with your access application.

6.3 Correcting your personal information

If you believe that the information the department holds about you is inaccurate, out of date, incomplete, irrelevant or misleading, you may ask for it to be corrected.

The department must make the correction unless there is a valid reason not to do so. If the department refuses to correct the information as requested, you can ask the department to place a statement with your personal information, setting out why you believe the information is inaccurate, out of date, incomplete, irrelevant or misleading.

6.4 More information

More information about how to apply for access to or correction of your personal information is available on the department's website.

If you still have questions about how to apply for access or correction of your information, the department's Information Access and Amendment Unit can assist you (contact details on last page of this policy).

7. Overseas transfer

As noted above, personal information collected by the department is generally held on servers located in Australia, either on-premise or in dedicated government tenancies in the cloud. The department retains effective control over all personal information held on the government cloud tenancy, and the information is handled in accordance with the QPPs.

However, personal information may be transferred overseas if, for example:

- you complete an online assessment which is processed overseas
- you complete a survey which is hosted overseas, or
- through web analytics or cookies.

You will be advised about any overseas transfer before you complete the survey or assessment, and if you do not want this to occur, please let us know and other arrangements will be made.

Web analytics and cookies may collect information about your device and browsing history, which is hosted overseas.

In very rare cases, back-up or technical support services may be provided from overseas. This will only occur in emergencies if there are no services available in Australia. The use or disclosure of personal information in those circumstances will be minimised.

8. Privacy breaches and complaints

The department has strong privacy and security processes to protect your information. However, a privacy breach may occur if personal information is not handled in accordance with the IP Act. Privacy breaches generally involve unauthorised access, use or disclosure of personal information.

8.1 Breach response

If the department becomes aware of a possible privacy breach, it immediately takes steps to:

- contain the breach
- evaluate the risks associated with the breach
- assess whether affected persons should be notified, and
- review what occurred and what action can be taken to prevent it happening again.

8.2 Complaint and review procedures

If you believe that your personal information has not been handled in accordance with the IP Act, you can contact the Complaints team to discuss your concerns or make a privacy complaint (contact details on last page of this policy).

Although generally the department accepts anonymous or pseudonymous complaints, if you want to make a privacy complaint, you will need to provide details of what information you believe was not dealt with in accordance with the IP Act. Therefore, it will not usually be possible to make a privacy complaint without providing identifying information. In addition, before we can discuss information about you, we need evidence of your identity, to ensure that your personal information is not used or disclosed inappropriately.

8.2.1 Making a privacy complaint

Generally, the department will only accept privacy complaints which are in writing and made within 12 months after you become aware of the matters you want to make a complaint about. Complaints made outside this time will only be accepted in exceptional circumstances.

You can use the Privacy complaint form to make a complaint. This form is also available in plain English. If you do not use the form, you must provide enough information to enable us to review the matter, including:

- your name
- evidence of your identity
- how we can contact you
- details of the act or practice you are complaining about, including when it occurred and what effect it has had on you, and
- what you want the department to do.

Privacy complaints should be marked ‘Private and confidential’ and forwarded to the Complaints address below. There is more information about the department’s complaint process on our website.

8.2.2 Complaints to the Office of the Information Commissioner

You may make a privacy complaint to the Office of the Information Commissioner (OIC) if:

- at least 45 business days have passed since you complained to the department and you have not received a response, or
- you have received a response but consider it is not an adequate response.

A complaint to the OIC must be made in writing, state an address to which notices can be sent, and give particulars of the act or practice complained of. If the matter is suitable for mediation, the OIC will take steps to resolve the matter.

However, the OIC will not deal with your complaint unless you have first made a complaint to the department. See the OIC website for details about its privacy complaints process.

8.2.3 Complaints to the Queensland Civil & Administrative Tribunal

If you are not satisfied with the outcome of the OIC mediation process, you may ask the OIC to refer the matter to the Queensland Civil and Administrative Tribunal (QCAT) for decision.

QCAT has published information about its privacy jurisdiction at Right to information and privacy jurisdictions of QCAT.

9. Contact details

Information Privacy

Telephone: (07) 3097 5609

Email: privacy@dcssds.qld.gov.au

Post: Information Privacy and Governance
Department of Families, Seniors, Disability Services & Child Safety
Locked Bag 3405
Brisbane QLD 4001

Information Access and Amendment

Telephone: (07) 3097 5605 or
1800 809 078 (Free call)

Email: rti@dcssds.qld.gov.au

Post: Information Access and Amendment
Department of Families, Seniors, Disability Services & Child Safety
Locked Bag 3405
Brisbane QLD 4001

Complaints Unit

Telephone: 1800 080 464

Email: feedback@dcssds.qld.gov.au

Post: Complaints Unit

Department of Families, Seniors, Disability Services & Child Safety
Locked Bag 3405
Brisbane Qld 4001

Appendix 1

Adoption

Adoption is a way to provide a permanent family for children who, for various reasons, cannot live with their birth family. The legal adoption process establishes a permanent parent-child relationship between a child and their adoptive parents. Adoption also removes the legal relationship between the child and their birth parents and extended family.

Adoption Services is responsible for providing services in Queensland for:

- parents considering adoption for their children
- children requiring adoptive placements
- people seeking to adopt children
- people seeking information or to lodge a contact statement in relation to a past adoption.

Adoption Services and Permanent Care Services provides services in accordance with the requirements of the *Adoption Act 2009* (Adoption Act) and the Adoption Regulation 2009. It is unlawful to attempt to privately arrange an adoption in Queensland.

How we manage your personal information

Adoption information can be sensitive and there are strong privacy and confidentiality protections that apply to Adoption information. However, there are also legislative processes that support the sharing of information. The Adoption Act authorises us to share some information, and other information is only shared with the consent of affected individuals.

More information about how we handle personal information is available at:

Adoption | Department of Families, Seniors, Disability Services and Child Safety

Changes to Queensland's adoption legislation - Access to adoption information

Changes to Queensland's adoption legislation - Removal of contact statement offence and penalty

Child and family services (child protection, family support, foster care)

The department is the Queensland Government's lead agency for child protection services, focused on the safety, belonging and wellbeing of children, and the delivery of services to build families' capacity to care for and nurture their children.

The department provides child protection and family support services. It is committed to enabling families to get the right support to care for their children and to protecting children and young people who have been harmed or are at risk of harm, and do not have a parent or carer able and willing to protect them. The department's role in protecting children and young people is to:

- arrange support services for families so they can safely care for their children and prevent the need for further intervention by the department
- assess concerns and determine whether a child is in need of protection
- provide ongoing intervention to children and young people who are experiencing, or are at risk of experiencing, significant harm, including services and care arrangements for children who cannot remain living at home

- fund non-government organisations to provide services directly to children, young people and families.

The department also provides adoption services for children and young people.

How we manage your personal information

There are strong privacy and confidentiality obligations that attach to child protection information. Information about how your personal information may be handled if you are involved with the child protection system is available at:

Information privacy | Department of Families, Seniors, Disability Services and Child Safety

Home | Child Safety Practice Manual

- ***Delegated Authority***

Most Aboriginal and Torres Strait Islander children live safely and happily with their families. However, due to the legacy of past policies and practices, Aboriginal and Torres Strait Islander children are disproportionately represented in the child protection system. In 2018, a suite of legislative reforms were made to the *Child Protection Act 1999* (the CP Act) which promote the safe care and connection of Aboriginal and Torres Strait Islander children with their families, communities and cultures, and support their self-determination.

The reforms provided the opportunity for Child Safety and Aboriginal and Torres Strait Islander Community-Controlled Organisations to adopt a new way of working and looking after the safety and wellbeing of children by putting culture and the aspirations of Aboriginal and Torres Strait Islander children and families first. This approach is grounded in a body of evidence that demonstrates connection and self-determination are critical to achieving better wellbeing outcomes.

In practice, this means that some decisions made and implemented by staff of the individual Child Safety Service Centres (CSSCs) can now be delegated to chief executive officers of Aboriginal and Torres Strait Islander Community-Controlled Organisations and implemented by these organisations. This enables children and families to be supported by Aboriginal and Torres Strait Islander Community-Controlled Organisations in partnership with staff from their local CSSC. The approach supports the safety, wellbeing and best interests of each child.

How we manage your personal information

If you are supported by a Aboriginal and Torres Strait Islander Community-Controlled Organisations through this arrangement, the department and the organisation may collect and share personal information about you as relevant to the particular functions the chief executive officer of the organisation is delegated to provide, in line with the requirements of the *Child Protection Act 1999*. Information is collected and shared in the interests of providing quality supports, assessing and meeting care needs and ensuring safety and wellbeing of each child.

However, there are strong privacy and confidentiality obligations that attach to child protection information. Information about how your personal information may be handled if you are involved with the child protection system is available at: xxx

- ***Office of the Child and Family Official Solicitor***

The Office of the Child and Family Official Solicitor (OCFOS) is an in-house legal unit within the department. Key responsibilities of OCFOS include:

- providing high quality legal advice and support to child safety service centres (CSSCs) in relation to the chief executive's statutory functions relating to the protection of children
- applying for emergency orders such as temporary assessment orders (TAO), court assessment orders (CAO) and temporary custody orders (TCO). This may include working with CSSCs to prepare applications, preparing submissions and appearing on matters, preparing case outlines, and assisting with appeals
- working with CSSCs to prepare briefs of evidence for child protection matters that are being referred to the Director of Child Protection Litigation (DCPL), and
- working with the DCPL to prepare matters for filing in the Children's Court.

How we manage your personal information

OCFOS does not generally collect personal information, but it does use and disclose personal information which the department holds to provide legal advice and conduct child protection litigation. OCFOS takes care to ensure that it only uses and discloses relevant information in court documents, and it has implemented extensive training and quality assurance processes for staff, to minimise the risk of unauthorised use or disclosure.

OCFOS conducts legal proceedings in relation to TAO, CAO and TCO applications. In doing so, it may file affidavits in court which it relies upon in support of those applications. This may involve the disclosure of personal information, but that disclosure is authorised under the *Child Protection Act 1999.* Any concerns about the disclosure of personal information in TAO, CAO or TCO proceedings should be raised with the department.

Where an application is brought for a child protection order, those legal proceedings are brought by the DCPL. The DCPL is an independent statutory agency, within the Department of Justice, which is responsible for applying for child protection orders on behalf of the State of Queensland and conducting the resulting legal proceedings in the Childrens Court of Queensland. The department is required and authorised to provide all relevant information to the DCPL to facilitate that process. The DCPL is responsible for the disclosure of information contained in court documents which it files and serves. The department frequently serves court documents on instructions from the DCPL. In doing so it is acting as an agent for the DCPL and any concerns about the disclosure of personal information in Child Protection Order proceedings should be raised with the DCPL.

Communities

The department oversees the implementation of the *Community Services Act 2007* (the CS Act) including the grants of funding to provide for assistance to service providers providing community services, and the regulation of the community services, and for other purposes.

The main object of the CS Act is to help build sustainable communities by facilitating access by Queenslanders to community services. The main object is achieved mainly by:

- the department giving financial and other assistance to service providers providing community services; and
- regulating community services provided with the financial or other assistance to ensure the standard and accountability of the services; and
- providing for compliance with the CS Act to be monitored and enforced.

Funding is provided under the CS Act only to services listed as a funding declaration. A declaration can apply the Act to a funding program or to individual funding contracts.

The Minister considers several factors when deciding whether to make a funding declaration, such as:

- the type of product or service being provided with the funding
- the importance of the product or service to meeting the needs of an individual, group or community
- the characteristics and vulnerability of users of the product or service
- the amount of funding being provided.

Note: issuing new Funding Declarations does not supersede or replace earlier declarations.

As community needs change, departmental investments will transition to meet these changes. Updated funding declarations will be made to safeguard our investments.

Funded organisations do not need to do anything to give effect to these declarations. Organisations' service agreements with the department continue and do not need to change. The terms and conditions of the *Community Services Act 2007* apply to the funding under the declaration and must be complied with by the organisation as applicable.

The Department of Communities, Housing and Digital Economy Funding Declaration 2022 (PDF, 73.13 KB) commenced 15 August 2022. This funding declaration applies the Act to all funding provided under Investment specifications approved by the Director-General.

How we manage your personal information

Communities only collects limited personal information, generally information about individuals applying for grants on behalf of service providers, which it uses to contact them in relation to their grant application. That information is managed in accordance with the IP Act.

Community Recovery

The department is the lead agency for Community Recovery, coordinating human and social recovery services when disasters such as floods, fires, cyclones, severe weather events such as monsoon troughs, and disease outbreaks occur in Queensland.

The response includes deploying the Community Recovery Ready Reserve workforce, mobilising community organisation and support services, delivering a network of Community Recovery Hubs across impacted communities, and administering personal hardship grants.

Community response operations occur directly before, during or immediately after a disaster to:

- save lives
- reduce health impacts
- ensure public safety, and
- meet basic subsistence needs of people affected.

Once a disaster area is deemed safety by emergency responders, the Ready Reserve can be deployed to start recovery operations.

Recovery

Community Recovery services help disaster-affected people by providing emotional support, material aid and financial assistance.

The Community Recovery Ready Reserve workforce of volunteers is comprised of public servants from across state government departments who have been approved for deployment. They help individuals and families with:

- practical information
- referral to support services, and
- access to financial assistance through grant applications.

More information is available at: What is Community Recovery? | For government | Queensland Government

How we manage your personal information

The department may collect personal information during an emergency, e.g. to identify whether individuals are at risk of harm, facilitate the provision of emergency services, and to provide financial and other assistance. As far as possible we will collect this information from you. However, in emergent situations this may not always be possible.

We may also share your personal information with other entities that can provide support or assistance. If we collect personal information (including financial information to facilitate payment of grants) from you, it will be collected and managed securely in accordance with the IP Act.

Disability Services

Disability Services is committed to fostering the social and economic inclusion of people with disability across Queensland. As part of our work, the department collects and manages personal information in compliance with Queensland and Commonwealth legislation.

The department collects personal information to deliver a range of disability services, including but not limited to:

- **Disability Accommodation Support and Respite Services:** Supporting National Disability Insurance Scheme (NDIS) participants through independent living and short-term accommodation requiring higher levels of care, such as 24-hour support.
- **Behaviour Support and Practice Quality:** Developing Positive Behaviour Support Plans to improve quality of life and manage behaviours of concern.
- **Restrictive Practice Operations:** Assessing and authorising the short-term use of restrictive practices for adults with intellectual or cognitive disabilities.
- **Guide, Hearing and Assistance Dogs:** Supporting individuals who rely on guide, hearing, or assistance dogs to access the community independently and ensures the quality and accountability of training services for these dogs.
- **Forensic Disability Services**: Providing therapeutic support in a medium-secure facility for individuals with intellectual disabilities who exhibit offending behaviours.
- **Assessment and Referral Team:** Offering intensive assistance to Queenslanders aged 7 to 64 years to access the NDIS and supporting young people with disability who are unable to live at home.

- **Queensland Specialist Disability Program (formally COS)** under 65 years of age who are ineligible for the NDIS.

How we manage your personal information

Disability Services is dedicated to managing personal information securely, transparently and accountably. Access to personal information is restricted to authorised staff and is used solely for purposes directly related to the provision of disability services and supports.

Data is securely stored in departmental systems such as Disability Accommodation Client Management Systems (DACMS), RESOLVE or iDOCS, with access restricted to trained and authorised staff.

Information is managed in compliance with legislation (such as the *Information Privacy Act 2009)* ensuring that the use of information aligns with legislative requirements and is not disclosed to third parties without lawful authority or consent.

If you have any questions or concerns about how personal information is managed, please contact us via disabilityenquiries@dcssds.qld.gov.au

Domestic and family violence prevention

Domestic and family violence (DFV) is an overt or subtle expression of a power imbalance, resulting in one person living in fear of another, and usually involves an ongoing pattern of abuse over time. DFV may take many forms ranging from physical, emotional, psychological, financial, monitoring and surveillance and other types of control, and it can have serious impacts on people who experience it.

The Queensland Government is leading a 10-year reform program to put an end to DFV in partnership with the non-government sector, business and the Queensland community. The reforms are making important investments and improvements across all sectors of DFV support, response and prevention.

The Queensland Government is working with our partners and the community to enable people to recognise, respond and refer effectively to prevent sexual, domestic and family violence to ensure the way we work supports people who have experienced violence and holds those responsible to account.

High Risk Teams (HRTs) are a core component of Queensland's integrated service response approach. HRTs are coordinated, multi-agency teams who provide integrated, holistic, culturally appropriate safety responses for victims and their children who are at high or imminent risk of serious harm or lethality.

HRTs consist of officers from agencies with a role in keeping victim-survivors safe and holding persons using violence to account, including police, health, corrections and housing staff along with specialist DV services.

How we manage your personal information

The department and all other members of the HRT are aware of the sensitivity of the information which is shared through this process. When matters are referred to a HRT, the members share relevant information to ensure that appropriate interventions to reduce harm and increase safety can be implemented.

As far as possible this information sharing is done with the victim-survivor's informed consent to ensure the safety and wellbeing of victim-survivors including children. At no time is the consent of the person using violence obtained, as this may increase the risk to victim-survivors.

In some cases, information provided to and by the HRT may indicate that a child is a risk of harm, and a referral to Child Safety will be made by the referring agency, if that has not already occurred. Information regarding child protection concerns shared with or at HRT does not negate any statutory obligations to report to Child Safety, nor is it the role of the Child Safety HRT member to report child protection concern information from HRT to Child Safety.

All relevant information which is shared with and by the HRT is stored in a departmental data base and accessed through a secure portal. Only approved HR members and departmental staff including Integration Managers are able to access the departmental database, with all approvals closely monitored by the department.

National Redress scheme

The National Redress Scheme was established in response to the Royal Commission into Institutional Responses to Child Sexual Abuse. The Commonwealth Government coordinates applications for redress under the scheme and sends requests for information to the department where it is named as the responsible institution. The department collates information from its records and prepares a response to the Commonwealth.

The department is also the central contact point for the Queensland Government, so it may also receive requests for information directed to other Queensland Government agencies. This occurs when the other agency has been named as a responsible institution or the department believes that the other agency holds information relevant to responding to a request for information from the Commonwealth. In those situations, the department coordinates the responses from the other agency and provides them to the Commonwealth.

The department may also be responsible for providing a direct personal response to applicants and facilitating counselling for applicants who choose these options.

How we manage your personal information

The department receives limited information from the Commonwealth in relation to the Redress applicant and uses that information to conduct searches and identify relevant information. The information is received, and responses are provided using a secure portal. Occasionally, information may be submitted via email (e.g. addendum responses).

The information is used and disclosed for purposes related to the Redress scheme. Information may be provided to the Queensland Government Insurance Fund, where that is relevant to a current civil claim. Information may also be disclosed for child safety purposes, for example, if an alleged abuser may be a current carer the information may be referred to the Regional Intake Service; or if the alleged abuser is a current employee, the matter may be referred to Professional Standards.

More information about how the department handles Redress information is available at Information privacy | Department of Families, Seniors, Disability Services and Child Safety

Seniors and carers

Seniors and Carers supports an age-friendly community where older people are valued, respected, and actively engaged in their community, they can stay in touch with people they care about and find the services and support they need.

The department works with other Queensland Government agencies to implement a range of age-friendly initiatives focusing on the opportunities and challenges of our ageing population and older people's issues. Those initiatives include:

- Queensland Government website for older people
- Seniors enquiry line and referral service
- Time for Grandparents information, respite and support
- Seniors Card scheme offering discounts on a range of goods and services
- Elder Abuse Prevention Unit (statewide telephone information support and referral)
- Seniors legal and support services, including free legal and social support services for seniors concerned about elder abuse, mistreatment and financial exploitation
- Social connection programs and activities with a focus on healthy lifestyle options, reducing social isolation and strengthening personal and community connectedness
- Council on the Ageing Queensland, the Queensland Seniors peak service, providing information on seniors' programs and services, working with other non-government organisations to improve the quality of services for older people and providing advice to government on seniors' issues.

Seniors and Carers team undertakes a comprehensive engagement program to support Queensland seniors. These events are designed to promote wellbeing, social participation, and cost-of-living relief while addressing region-specific issues through direct engagement and pulse surveys. These initiatives include Seniors Expos, Seniors Savings Pop-Ups and Seniors Connect Newsletter.

Seniors and Carers collaborates with stakeholders to deliver events and information that empower older people to lead healthy, productive, and socially connected lives. Key initiatives are outlined in the Queensland Seniors strategy 2024-2029.

Seniors and Carers also provides secretariat support to the Queensland Carers Advisory Council which provides strategic advice on work to promote the interests of unpaid carers and makes recommendations to support carer recognition.

How we manage personal information

Digital Customer - Smart Service Queensland (SSQ) which sits within the Department of Customer Service, Open Data and Small and Family Business is responsible for the operational service delivery of schemes (e.g. Seniors Card Scheme, Carer Business Discount Scheme, Companion Card, Medical Cooling and Heating Electricity Concession Scheme, Electricity Life Support Concession Scheme and Home Energy Emergency Assistance Scheme) for the department.

The business discount aspect of the Scheme is a partnership between the Queensland Government and participating businesses to provide discounts on a range of products and services. The card schemes do not share personal details of cardholders with businesses.

Applicants may be required to provide identification and eligibility documents where appropriate. This information may be shared with other government agencies (e.g. Department of Transport and Main Roads, Services Australia and Department of Veterans' Affairs) to verify eligibility.

Information may be shared with third parties for correspondence and card delivery. All Queensland Government agencies involved in delivering the cards collect, store, use and disclose personal information in accordance with the Queensland privacy principles in the *Information Privacy Act 2009* (IP Act).

The department may contact applicants from time to time to advise about the program, benefits and any changes. Cardholders may nominate to receive relevant information, including available concessions, events and programs. If you no longer wish to receive this information you can update your contact preferences by calling 13QGOV (137468).

Applicants to join the Queensland Carers Advisory Council may be required to provide documents to confirm their eligibility for membership of the Council. Information may be shared with Queensland State Library Queensland to enable completion of a Government Research and Information Library (GRAIL) check during the Council recruitment process.

The department provides the names of recommended appointees to the Minister for Families, Seniors and Disability Services and Minister for Child Safety and the Prevention of Domestic and Family Violence, and the Premier of Queensland through the Department of Premier and Cabinet. The names of successful applicants may be published in a media release with consent.

All information obtained in the Council nomination and assessment process and in administration of the Council is managed by the Department and other Queensland Government agencies in accordance with the *Information Privacy Act 2009* (IP Act).

Corporate services

Corporate services supports the delivery of all of these services by providing strategic leadership and direction for the department's corporate systems, policies, and practices.

Corporate Services supports departmental staff by:

- delivering learning and development opportunities
- equipping them with better technologies
- running effective financial, funding and procurement, and human resource systems
- providing legal services and advice
- reporting and analysing data
- undertaking audit, compliance, and other reviews
- handling complaints, investigations, and information access requests, and
- managing our facilities and delivering our capital projects.

How we manage your personal information

Corporate Services collect, use and disclose personal information in order to:

- support staff training and development
- ensure that staff have access to appropriate technology and supports
- ensure that information holdings are securely maintained and disposed of in accordance with legislative obligations
- facilitate prompt and accurate payment and access to leave entitlements
- support planning and delivery of service improvements
- ensure appropriate facilities and manage our facilities
- respond to complaints, investigations and information access requests.