



Parliamentary Service Privacy Policy

Effective date: October 2010

Last updated: August 2012

Authority

The authority for the Information Standards and Policies contained in this document is derived from the *Parliamentary Service Act 1988*, in particular the authority of the Committee of the Legislative Assembly (CLA) to make and determine policies for the Parliamentary Service under s.6 of the Act. As agreed to on 7 September 2011, the CLA delegated the management and review of the Parliamentary Service Privacy Policy to the Clerk.

Privacy Policy

1. Introduction

The [Information Privacy Act 2009](#) (IP Act) regulates how public sector agencies, the Parliamentary Service, Ministers and statutory bodies must manage personal information. It creates an obligation to comply with the privacy principles, which include the Information Privacy Principles (IPPs), the conditions under which personal information may be transferred outside of Australia and the rules regarding contracted service providers.

Further information may also be accessed at the [Office of the Information Commissioner](#) website.

1.1 Who needs to know the requirements of the IP Act?

The Parliamentary Service Privacy Policy (PPP) applies to:

- Parliamentary Service officers and employees;
- Electorate office staff (in a limited sense, when acting as a Parliamentary Service employee and NOT when acting as an agent of the Member); and
- Contractors and consultants to the Parliamentary Service.

The policy does not apply to:

- The Legislative Assembly;
- Members of Parliament and their electoral office staff (when acting on specific or general instructions from the Member to whom they are assigned);
- Committees of Parliament; and
- Parliamentary Proceedings that are kept by the Parliamentary Service.

A member of Parliament may decide to subscribe their electorate office to the Privacy Policy.

2. Application of the Privacy Policy

2.1 Parliamentary officers and employees

When dealing with personal information, Parliamentary officers and employees will comply with the Information Privacy Principles outlined in this policy.

2.2 Electorate officers when acting as Parliamentary Service employees

Schedule 2 of the Act clearly exempts Members of the Legislative Assembly from complying with the Information Privacy Principles (IPPs). Therefore, Electorate Office Staff will not be bound by the Act when acting on behalf of the Member. However, the Parliamentary Service is not exempt from the operation of the Act (see 2.1 above). This means that the Act may apply to Electorate Office Staff in a limited capacity as employees of the Parliamentary Service.

2.3 Contractors and Consultants to Queensland Parliament

The Parliamentary Service may:

- Engage consultants directly to perform a specific function; and/or
- Contract services in whole or in part to a contractor.

Consultants and Contractors must abide by the requirements of the IP Act under the terms of their contracts with the Parliamentary Service.

2.4 The Legislative Assembly, its Members and Committees

By virtue of section 9 of the *Constitution of Queensland Act 2001*, the Legislative Assembly has the powers, privileges and immunities of the House of Commons. The privileges of Parliament exist to enable the Parliament (including its Members and Committees) to proceed with its business without interference or molestation and to protect it against unwarranted attacks upon its authority. Amongst its many privileges is the right to control its own proceedings, including the right to order the publication and non-publication of its proceedings and the manner in which it keeps its records. "Proceedings in the Assembly" is defined in the *Parliament of Queensland Act 2001* and includes evidence given before the Assembly or a committee of the Assembly or a document laid before, or presented or submitted to, the Assembly, a committee or inquiry.

How personal information collected by the Legislative Assembly, its Members and Committees is dealt with is regulated by standing rules and orders. For example: Standing Orders 211 and 211A provide:

211. Confidentiality of proceedings for Portfolio Committees and the Committee of the Legislative Assembly
- (1) The proceedings of a portfolio committee, the Committee of the Legislative Assembly Committee or a select committee or a subcommittee of any of those committees that is not open to the public or authorised to be published remains strictly confidential to the committee until the committee has reported those proceedings to the House or otherwise published the proceedings.
 - (2) Paragraph (1) does not prevent-
 - (a) The disclosure, by a committee in (1) or by a member of the committee or an officer of the committee, of proceedings to a member of Parliament or to the Clerk or another officer of the House in the course of their duties;
 - (b) a public servant or an officer of a public entity informing their immediate supervisor, Director-General or Chief Executive Officer, or responsible Minister of the evidence they have provided to a committee in (1) or evidence sought by a committee; and
 - (c) The disclosure of proceedings otherwise in accordance with these Standing Orders
 - (3) Despite (2), a committee in (1) may resolve that some or all of its proceedings relating to an inquiry or report remain confidential to the committee, its members and officers until it reports to the House on the inquiry.
 - (4) Despite (2), no member shall in the House refer to any proceedings of a committee in (1) until the committee has reported those proceedings to the House or otherwise published the proceedings.
- 211A. Confidentiality of proceedings for Parliamentary Crime and Misconduct Committee and Ethics Committee
- (1) The proceedings of the Parliamentary Crime and Misconduct Committee and the Ethics Committee or a subcommittee of those committees that is not open to the public or authorised to be published remains strictly confidential to the committee until the committee has reported those proceedings to the House or otherwise published the proceedings.
 - (2) No member shall in the House refer to any proceedings of a committee in (1), until the committee has reported those proceedings to the House or otherwise published the proceedings.
 - (3) A member who wishes to refer to in camera evidence or unpublished committee documents of a committee in (1) in a dissenting report shall advise the committee of the evidence or documents concerned, and all reasonable effort shall be made by the committee to reach agreement on the disclosure of the evidence or documents for that purpose.
 - (4) A committee in (1) may elect for this Standing Order to not apply to a particular proceeding or a particular inquiry of the committee, and adopt its own rules in relation to the confidentiality of its proceedings for that proceeding or inquiry.

A breach of Standing Order 211 or 211A may constitute contempt of Parliament.

A Member of Parliament must deal with information in a way that does not violate the Standing Orders. The PPP cannot and does not purport to regulate how Members of Parliament deal with information that comes into their possession. However, Members are free to inform themselves of the requirements of the PPP and may choose to comply with the IPPs and apply it in their electorate office where it is appropriate for them to do so.

3. Personal Information

3.1 What is personal information?

The IP Act defines personal information 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. For example: addresses, phone numbers, medical details and financial details.

Personal information may be contained in (but is not limited to) the following:

- Paper records;
- Electronic records;
- Digital recordings;
- Digital images; and
- Photographs.

Personal information is not limited to information that is sensitive or confidential, although the degree of sensitivity or confidentiality may influence the way in which the IPPs are applied in particular circumstances. Many of the IPPs require that reasonable actions be taken, having regard to the specific circumstances and the nature of the information. As such, procedures may vary with the sensitivity of the information.

3.2 What is not personal information?

Personal information does not include information about a person that is already contained in a publicly available publication, such as magazines, books, newspapers, newsletters, annual reports and the Queensland Government Gazette. Although personal information about a deceased person is not technically considered to be personal information, Queensland Parliamentary Service officers and employees are encouraged to respect the sensitivities of family members when using this information.

3.3 Personal Information collected by the Parliamentary Service

The Queensland Parliamentary Service (QPS) collects personal information about:

- Members of Parliament and related persons;
- QPS officers and employees and prospective officers and employees;
- QPS suppliers;
- QPS catering clients;
- QPS contractors and tradesmen;
- Visitors to Parliament; and
- Subscribers to Parliamentary publications and services.

Parliamentary Committees may collect personal information in the course of their inquiries.

4. Information Privacy Principles

There are 11 Information Privacy Principles contained in the IP Act. The IPPs specify how personal information is to be collected, stored, secured, accessed, amended, used and disclosed.

Collection

IPP1 – Limits the scope of the collection and the way in which an agency collects.

IPP2 – Requires agencies to give individuals notice about the purpose of the collection, disclosures and subsequent disclosures (*e.g. forms for collecting names and addresses should give notice if personal information is likely to be passed on to a 3rd party*).

IPP3 – Requirements regarding relevance and recency of information collected and way in which an agency collects (*e.g. full addresses should only be asked for where necessary and reasonable steps should be taken to keep databases up to date*).

Storage and Security

IPP4 – Requires:

- Protection against loss, unauthorized access use, modification or disclosure and any other misuse (*e.g. personal information should be securely stored*).
- Prevention of unauthorized use or disclosure of personal information by contractors (*e.g. contracts with 3rd parties to build a database involving personal information should include a privacy clause*).

Access and Amendment

IPP5 – Publication of information about agency's personal information holdings (*the Privacy Officer will centrally coordinate this across the parliamentary service*).

IPP6 and 7 – Access to documents containing the personal information by the individual to whom the information relates and the accuracy and correction of that information (*e.g. individual's can request access to the Parliamentary Service records containing their personal information*).

Use

IPP8 – Ensuring information is accurate, complete and up-to-date before using it.

IPP9 – Use only the parts of the personal information directly relevant to fulfilling the particular purpose.

IPP10 – Limit on use.

IPP10(1) – An agency must not use personal information for a purpose other than the particular purpose for which the information was obtained unless one of the exemptions in paragraphs (a) to (f) apply:

- (a) likely awareness (*e.g. if a member of the public attends a public hearing at parliament where there are photographs being taken, the individual should be likely aware that their image may be used in the Committee's report in relation to that hearing*).
- (b) prior agreement
- (c) serious threat to health, safety or welfare
- (d) required or authorised under a law
- (e) law enforcement
- (f) research and statistics.

Disclosure

IPP11- an agency must not disclose personal information to an entity (other than the individual the subject of the personal information) unless one of the exemptions in paragraphs (a) to (f) apply:

- (a) likely awareness
- (b) prior agreement
- (c) serious threat to health, safety or welfare
- (d) required or authorised under a law
- (e) law enforcement
- (f) research and statistics

IPP11(3) – all reasonable steps to ensure that recipient will not use or disclose the information for another purpose.

IPP11(4) – additional limitation on disclosure where the information may be used for marketing to the individual.

5. Exempt personal information

The following personal information is exempt from the IP Act:

5.1 Covert activity

A document to the extent it contains personal information:

- Arising out of or in connection with a controlled operation or controlled activity under the *Police Powers and Responsibilities Act 2000* or the *Crime and Misconduct Act 2001*.
- Arising out of or in connection with the covert undertaking of an operation, investigation or function of a law enforcement agency.
- Obtained under a warrant issued under the *Telecommunications (Interception and Access) Act 1979 (Cwth)*.

5.2 Witness protection

A document to the extent it contains personal information about a person who is included in a witness protection program under the *Witness Protection Act 2000* or who is subject to other witness protection arrangements made under an Act.

5.3 Disciplinary actions and misconduct

A document to the extent it contains personal information arising out of:

- A complaint under the *Police Service Administration Act 1990*, part 7.
- A complaint, or an investigation of misconduct, under the *Crime and Misconduct Act 2001*.
- An investigation of misconduct under the *Parliamentary Service Act 1988*.

5.4 Public Interest Disclosure

A document to the extent it contains personal information:

- Contained in a public interest disclosure under the *Public Interest Disclosure Act 2010*.
- That has been collected in an investigation arising out of a public interest disclosure under the *Public Interest Disclosure Act 2010*.

5.5 Commissions of Inquiry

A document to the extent it contains personal information arising out of a commission of inquiry.

5.6 Cabinet and Executive Council

A document to the extent it contains personal information that is also the subject of the *Right to Information Act 2009* (Qld), schedule 3, section 1, 2 or 3.

5.7 Generally available publications, archives and posted articles

A document that is:

- A generally available publication.
- Kept in a library, art gallery or museum for the purposes of reference, study or exhibition.
- A public record under the *Public Records Act 2002* in the custody of Queensland State Archives that is not in a restricted access period under that Act.
- A letter, or anything else, while it is being transmitted by post.

6. Responsibilities for Privacy in the Parliamentary Service

The overall responsibility for privacy in the Parliamentary Service resides with the Clerk of the Parliament. The responsibility for the day-to-day management has been delegated to the Parliamentary Service Privacy Officer.

The Parliamentary Service Privacy Officer is the first point of contact for members of the public and officers 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 Parliamentary Service.

The Privacy Officer can be contacted on 3406 7167.

The Privacy Officer is responsible for reporting privacy matters to the Clerk of the Parliament and for preparing relevant statistical reports for senior management and for inclusion in the Parliamentary Service's annual report.

7. Classes of personal information held

A personal information audit was undertaken that allowed the Parliamentary Service to identify and record those datasets that contain personal information. At paragraph 10 is the name of each dataset identified, a description of personal information in the dataset, details relating to the relevant retention period and the authorised staff who have access and use of that personal information.

8. Access and amendment procedures

Parliamentary Service officers and employees can access and amend their personal information by contacting the Human Resources Manager.

9. Review procedures

If you believe that your personal information has **not** been dealt with in accordance with the Parliamentary Service's obligations under the IP Act, you may make a complaint in writing to the Parliamentary Service. This complaint must be made within 12 months from the date that you first became aware of the act that is the subject of the complaint.

Complaints should be forwarded to:

Privacy Officer
Ethics Committee
Queensland Parliament
Brisbane Qld 4001

Complaints will be acknowledged in writing within 5 business days from the date on which the complaint was received and processed within 45 business days. The complainant will be advised in writing of the decision, including any remedies that are considered appropriate to resolve the complaint.

If an applicant does not agree with a decision, they can apply in writing to the Clerk of the Parliament who will appoint a panel to conduct an internal review of the initial decision. Applications for an internal review must be made within 28 days of the complainant receiving the first decision notice.

The internal review will be completed within 45 business days of receipt of the application for that review and you will be advised of the outcome of this decision.

If the applicant does not receive a decision on the complaint within the specified timeframe, or is not satisfied with the decision, the applicant may make a complaint to the Information Commissioner. The Information Commissioner will try to resolve the complaint through mediation.

If the complaint cannot be resolved through mediation, the applicant may direct the Information Commissioner to refer the complaint to the Queensland Civil and Administrative Tribunal (QCAT).

10. Personal Information Digest

10.1 Personnel records

Due to the commonality of these classes of records amongst the service areas and units of the Parliamentary Service, employee personnel records have been grouped here as one entry. Current and former officers and employees and other persons (for example, spouses and next of kin who believe that the Parliamentary Service's personnel records may also contain personal information about them) can obtain details of specific record handling practices by contacting the Human Resource Management Service. It should not be assumed that all records described are kept in a common storage facility. Separate security arrangements will typically apply, depending on the sensitivity of the information.

The purpose of employee personnel records is to maintain employment history and payroll and administrative information relating to all permanent, contract and temporary staff members and officers and employees of the Parliamentary Service.

Those records also facilitate the recruitment function of the Human Resource Management Service. Personal information about applicants for employment within the Parliamentary Service is used solely for the purpose of selecting officers and employees and can be accessed by members of selection committees and staff responsible for approving appointments.

10.1.1 Personnel and Payroll

The records relating to current and former staff members and officers and employees including contract and temporary staff may include any one or more of the following—

- records containing details such as name, address, home telephone number, mobile telephone number, e-mail address, date of birth, occupation, employee identification number, gender, qualifications, next of kin, emergency contact person and telephone number;
- records relating to attendance and overtime;
- leave applications and approvals;
- medical records;
- payroll and pay related records, including banking details for EFT payments;
- tax file number declaration forms;
- declarations of pecuniary interests;
- superannuation details;
- personal history files;
- performance appraisals;
- records relating to personal development and training;
- records relating to removals;
- travel documentation; and
- records relating to personal welfare matters.

10.1.2 Recruitment

The records may include any one or more of the following—

- records relating to the selection and recruitment of staff;
- records relating to relocation of staff and removals of personal effects; and
- records relating to character checks and security clearances.

10.1.3 Other Employment Records

The records may include any one or more of the following—

- records of accidents and injuries;

- compensation case files;
- rehabilitation case files;
- records relating to counseling and discipline matters, including disciplinary, investigation and action files, legal action files, records of criminal convictions, and any other staff and establishment records as appropriate;
- complaints and grievances; and
- recommendations for honours and awards.

Contents of the above personnel records may include information about 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 clearance details and employment history; physical and mental health, disabilities, racial or ethnic origin, disciplinary investigations and action, criminal convictions, adverse performance and security assessments, relationship details and personal financial information.

The following staff have access, as appropriate, to the above records: Human Resources Management Services staff, the Clerk of the Parliament and Managers of Service Areas in relation to staff in their relevant areas; Members of Parliament (to information of their Electorate Office staff); and the individual to whom the record relates.

Information held in personnel records may be disclosed to third parties outside the Parliamentary Service, as appropriate, including: the Australian Taxation Office; QSuper; Centrelink; WorkCover Queensland; Public Service Commission; and third parties, such as banks and insurance companies (name and account numbers only). Otherwise, information is only disclosed to third parties with the permission of the staff member or as required by law.

Individuals can obtain information regarding access to their personal information by contacting the Manager, Human Resources Management Services on 3406 7544.

Personnel records are kept for variable periods and stored in paper and electronic form located in-house. Old payroll data are archived at CITEC.

10.2 Staff Contact Lists

Electronic and paper records are widely held within the Parliamentary Service by staff members to enable emergency contact of staff and for other staff management purposes such as to contact casual or contract staff when work is available; to enable Parliamentary Security Services to fulfill their internal security functions including responding to emergency situations.

Records of contact details (including names, addresses and telephone numbers) of tradespersons and contracted Department of Public Works Field Staff are also maintained for the purpose of facilitating 24 hour contact with those persons and also to enable the Parliamentary Security Service to allow entry to the Precinct and provide an escort service to contractors working after business hours. Similar contact details for individuals who perform casual and contract work for relevant Service areas are also maintained for the purpose of enabling contact when those persons' services are required.

Contents of staff contact lists may include names and addresses, mobile and home contact telephone numbers.

The following staff have access, as appropriate, to the above records: Managers and Supervisors in Service areas to which the staff contact details relate and other authorised staff in those areas. The information is not generally disclosed to other persons or organisations outside the Parliamentary Service.

Records are kept for variable periods and stored in paper and electronic form located in-house.

10.3 Supplier and Client Contact Lists

The Parliamentary Service maintains supplier and client contact lists, mailing lists, and collects business cards for a range of business reasons. Those include placing orders and invoicing.

General content may include names, addresses and telephone numbers of individual service providers, suppliers and potential suppliers of goods and services to the Parliamentary Service.

The personal information is used only to facilitate the supply of and payment for goods and services.

The following staff have access, as appropriate, to this information: the Catering Manager, Duty Manager and Executive Chef, the Property Services Manager, Electorate Accommodation Officer, Maintenance Supervisor and House Supervisor. The staff of Financial Services are entitled to access this information as part of financial management functions. Staff within Property Services and Parliamentary Security Services may have access to some personal information contained in a staff distribution list. The information is not generally disclosed to other persons or organisations outside the Parliamentary Service.

Records are kept for variable periods and stored in paper and electronic form located in-house.

10.4 Mailing Lists

The purpose of mailing list records is to enable individual service areas within the Parliament Service to provide individuals with requested information on an ongoing basis and to keep individuals informed of various matters. For example, the Parliamentary Reporting Service uses mailing lists to furnish individuals who have requested a copy of Hansard with that publication in a hard copy format. The Parliamentary Library uses mailing lists to distribute research briefs and reports prepared by library staff.

General content of mailing lists may include names and addresses of interested individuals.

The following staff have access to this information: all staff, including Parliamentary Reporting Services staff (Hansard), who are involved in generating mailing lists and involved in the distribution of information to individuals on those lists and to electorate officers who may supply the information originally. The information is not usually disclosed to other persons or organisations.

The records are kept for variable periods and stored in paper and electronic form.

Individuals can obtain information regarding access to their personal information by contacting the relevant section of the Parliamentary Service.

10.5 Financial Management Information

There is a commonality amongst these records across the service areas of the Parliamentary Service so they are grouped here as one entry.

The purpose of these records is to process and account for expenditure and revenue. It is also for the purpose of the administration of members' and former members' entitlements, including travel arrangements.

Contents of financial management information may include: name, address and service or goods category; and financial information. Sensitive content may include financial information including debts. Personal information may include service providers' personal contact details and personal financial details such as banking details for EFT purposes.

The following staff have access to this information: Financial Services staff who are authorised by the Manager of Financial and Administrative Services. There is also disclosure, on occasion, of some Members' personal information to Human Resource Management Services to facilitate payments of salary. Disclosure to third parties is not usual apart from providing some Members' personal details to Government agencies and private organisations for the purposes of facilitating travel arrangements for Members.

The records are kept for variable periods and stored in paper and electronic form.

Individuals may obtain information regarding access to their personal information by contacting the Manager of Financial and Administrative Services on 340 67488.

10.6 Visitors' Book

A Visitors' Book is kept for security reasons to record names and addresses of members of the public who visit Queensland Parliament.

Contents of the Visitors' Book may include names and addresses of individuals.

Any member of the public can have access to their personal information contained in the Visitor's Book by contacting Manager Security & Attendant Services on 340 67115.

10.7 Information Systems Records

The Parliamentary Service information technology 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 Parliamentary Service on behalf of the Service areas.

It encompasses both internal electronic transactions and external transactions, including telephone, e-mail, Internet and government Intranet activity. The great bulk of those personal information records within that network environment are described above, or are described in the other parts of this plan that deal with the content of core business operations of the Parliamentary Service. This extends to all individual and whole of Parliamentary Service e-mail address groups.

In addition to that material, there are some personal information records specifically tailored to IT system administration, namely IT system security identifiers and usage tracking records about staff users of IT systems that are held by central IT administrators and staff supervisors.

Information described above is not usually disclosed to persons other than staff supervisors, system administrators and the individual officers concerned. IT administrators are authorised to access the transaction logs to carry out work sufficient to satisfy network security and audit requirements. Staff are routinely made aware of system usage rules and monitoring procedures concerning collection and use of the information. The records are not usually disclosed to other persons or organisations.

The Parliamentary Library also keeps records of usage of research and information services and electronic databases by members, electorate offices and Parliamentary staff but only the Librarian and Library management have authority to access those records of usage.

Individuals can obtain information regarding access to their personal information by contacting the Manager of Information Technology Services on 340 67478.

10.8 Database of Members' Details

The Parliamentary Service maintains a comprehensive database of Members' details.

Contents of that database of Members' details may include personal addresses, phone numbers, spouse name, banking details, airline membership details of members.

The following staff have access to this information: the Executive Secretary to the Director of Corporate and House Services (and the IT Project Officer while database under construction). Some personal information may be disclosed to Human Resource Management Services where there is advice of a change of contact details. The information is not usually disclosed to other persons or organisations.

The records are kept for variable periods and stored in paper and electronic form on equipment located in-house. It is archived on IT networks.

10.9 Driver's Licence Details

Driver's licence information (i.e. a photocopy of individuals' drivers' licences) is collected by the Parliamentary Service from those who drive official parliamentary vehicles, for motor vehicle policy and insurance requirements and for tracking traffic infringements.

The following staff have access to this information: the Manager of Financial and Administrative Services, Executive Secretary to the Director of Corporate and House Services, the Speaker's Executive Officer, and Director of Corporate and House Services.

Information held in personnel records may be disclosed to third parties outside the Parliamentary Service, as appropriate, including: QFleet and/or agencies concerned with traffic infringements, such as the Department of Main Roads. The information is not usually disclosed to other persons or organisations.

The records are kept for variable periods and stored in paper and electronic form on equipment located in-house. They are shredded when no longer required.