



DPS Privacy Policy

Policy Summary	
Status	Version 1.0 Current as of October 2022.
Purpose	This policy sets out how the Department of Parliamentary Services (DPS) collects and uses personal information; how the information is stored, accessed and privacy protected; and provides information on the recourse available to individuals who believe that information has been handled inappropriately.
Scope	<p>This policy applies to personal information collected, stored, accessed, and used by the Department of Parliamentary Services. This policy refers to personal information relating to members, staff and the public.</p> <p>The policy does not cover CCTV information as the use, storage, access and disposal is covered in detail in the Closed Circuit Television (CCTV) and Security Access Control Systems (NSW Parliament House) Policy.</p> <p>This policy does not cover records created by the Departments of the Legislative Assembly and Legislative Council, or members and their staff, which may contain person information. Where providing any information that may breach parliamentary privilege the advice of the relevant Clerk will be sought.</p>
Availability	This policy is available on the Parliament's intranet and website.
Policy owner	The Chief Information Officer, DPS is responsible for administering the communication, maintenance and revision of this policy.
Related policies & documents	<p><i>Privacy and Personal Information Protection Act 1998</i></p> <p><i>Health Records Information Privacy Act 2002</i></p> <p>Closed Circuit Television (CCTV) and Security Access Control Systems (NSW Parliament House) Policy</p> <p>Parliament House Security Pass Policy</p> <p>IT Access and Use Policy</p> <p>IT Operations Policy</p> <p>Cyber Security Policy</p> <p>Public Interest Disclosures Policy (DPS)</p> <p>See section 7.0 of this document for a full listing of related legislation and policies.</p>
Policy review	This policy must be reviewed once each Parliament, or as required in response to changes in legislation and/or regulation.
Approval	Mark Webb, Chief Executive, Parliamentary Services
Date	12 October 2022



Table of Contents

1.0 Purpose	3
2.0 Scope	3
3.0 Definitions	3
4.0 Policy	5
4.1 Roles and Responsibilities.....	5
4.2 Collection	5
4.3 Storage.....	7
4.4 Access and Accuracy	7
4.5 Use.....	8
4.6 Disclosure to relevant authorities.....	8
5.0 Grievance mechanisms/sanctions.....	9
6.0 Accountabilities	9
7.0 Related policies, legislation, guidelines and forms	9
8.0 Policy review.....	10
9.0 Further information	10
10.0 Document control.....	10



1.0 Purpose

This policy articulates how the Department of Parliamentary Services (DPS) meets the Information Protection Principles (IPPs) outlined in the *Privacy and Personal Information Act 1998*.

The policy sets out how DPS

- Collects and uses personal information within the processes and systems of DPS
- Stores, secures and protects personal information held
- Enables people to access and correct their own personal information
- Provides information on how personal information can be disclosed and to whom
- Provides information to individuals who believe that information has been handled inappropriately.

2.0 Scope

This policy applies to personal information collected, stored, accessed, and used by the Department of Parliamentary Services. This policy refers to personal information relating to members, staff and the public.

The policy does not cover CCTV information as the use, storage, access and disposal is covered in detail in the Closed Circuit Television (CCTV) and Security Access Control Systems (NSW Parliament House) Policy.

This policy does not cover records created by the Departments of the Legislative Assembly and Legislative Council, or members and their staff, which may contain personal information. Where providing any information that may breach parliamentary privilege the advice of the relevant Clerk will be sought.

3.0 Definitions

DPS means the Department of Parliamentary Services.

Department Head means the Clerk of the Parliaments, Clerk of the Legislative Assembly or the Chief Executive, Parliamentary Services.

Health Information is a specific type of 'personal information', which may include information about your physical or mental health or disability which you provide to any health organisation or Parliament of NSW.

IPPs means Information Protection Principles.



Parliament means the Parliament of New South Wales.

Personal Information is any information that identifies a person (members of the public and staff) including:

- A record, which may include your name, address and other details about you
- Photographs, images, video or audio footage
- Biometric identification like fingerprints
- Sensitive information e.g. conduct/performance reports.

PIIP Act means the *Privacy and Personal Information Protection Act 1998*.

Record means information created or received in the course of a parliamentary department's administrative and parliamentary business, which:

- evidences a decision
- approves or authorises actions
- constitutes formal communications between staff or with people outside the Parliament
- signifies a policy change or development, or
- commits the Parliament to an arrangement or business deal.

Records can exist in various forms including paper, digital, photographic, video, micrographic and audio.

Third Party is a person or group besides the two primarily involved in a situation, especially a dispute.



4.0 Policy

4.1 Roles and Responsibilities

- a) **The Chief Executive DPS** is responsible for ensuring:
 - complaints and suspected breaches are investigated
 - authorising access and disclosure requests
 - assuring compliance with this policy in DPS.
- b) **The Chief Information Officer** is responsible for administering the communication, maintenance and review of this policy.
- c) **The business owners of systems** containing personal information of staff, members and the public are responsible for implementing appropriate systems and processes to maintain and protect personal information in accordance with this policy.
- d) **Other Executive Directors, Directors, Senior Managers and supervisors** are responsible for, and must monitor, the compliance of this policy in their work areas.
- e) **DPS staff** are responsible for capturing, using, maintaining and storing personal information in accordance with this policy. They must report to their supervisors any breaches or suspected breach of this policy.

4.2 Collection

DPS will only collect and hold information that is reasonably necessary for the proper performance of the functions and services provided by DPS or as required by legislation.

Wherever possible, DPS will collect this personal information directly from individuals or organisations which may include (but is not limited to) the following:

- Contact details such as name, address, telephone number and email address
- Personal identification credentials such as photographs, driver's license, passport
- Recruitment information such as education and qualification credentials and current employment information
- Workplace information such as reference checks, performance reviews, absence from work certificates, statements of illness on leave forms, psychological reports and medical reports in association of any workers compensation claims
- Financial information including bank and superannuation account details, tax file number and payroll details
- Photographs/images for security passes and workplace communication



Parliament of New South Wales Policy Series

- Police and working with children check clearances
- Information about incidents in the workplace
- Personal information gathered during monitoring of IT systems for inappropriate use of systems.

Information is collected using a variety of methods including but not limited to forms, interviews, meeting notes, emails, file notes, resumes and job application documentation.

Personal information may also be collected automatically while accessing one of the NSW Parliament's website or intranet pages. When anyone visits webpages on these sites, their computers automatically transmit information that identifies, for each page accessed:

- the IP (Internet Protocol) address of the machine that has accessed it
- the visitor's top-level domain name (for example .com, .gov, .au, .uk etc.)
- the address of visitor's server
- the date and time of the visit to the site
- the pages accessed and documents downloaded
- the previous site visited, and
- the type of browser and operating system used.

This information may be analysed by the Parliament for research and audience analysis using Google Analytics. Cookies may remain on the enquirer's browser history.

Users of the NSW Parliament websites and intranet are entitled to expect that any information collected as a result of that use will be treated within the terms of this policy.

The Privacy Policies for Parliament's websites are located at

<https://www.parliament.nsw.gov.au/pages/privacy-statement.aspx> and
<https://parliamentarycatering.com.au/privacy-policy>

Personal information may also be collected through third parties including:

- Educational institutions and training providers
- Medical practitioners
- Previous or current employers and nominated referees
- Criminal records check providers
- Publicly available sources including newspapers, journals, directories, the internet and social media sites.

Collected information will be managed in accordance with the *PPIP Act* and our Privacy Policy.



4.3 Storage

Personal information is held in DPS's information systems until it is no longer required for its given purpose, at which time it will be de-identified and/or destroyed in line with the PIPP legislation.

All personal and confidential information held by DPS is stored securely and protected from unauthorised use or access in systems with audit and monitoring functionality. Controls are in place to ensure limited access to this information, with access provided only to those staff with a direct responsibility for maintaining and monitoring the information. The Information is stored with appropriate security measures in place for both digital and hardcopy formats. These measures include use of locked cabinets and storage rooms, security classifications and security access groups within the corporate records management system.

Records containing personal information are maintained until they are disposed of in accordance with the General and Functional Disposal Authorities issued by State Archives and Records under the State Records Act and in accordance with the Parliament's Records Management Policy.

4.4 Access and Accuracy

DPS is committed to taking reasonable steps to ensure that the personal information held is accurate, up to date and complete.

An individual can gain access to their personal information held by DPS to ensure that it is accurate, complete and up to date.

For security purposes, individuals are asked to request in writing and may need to verify their identity before information is released. DPS will respond to requests for access within 14 days. DPS may refuse to provide access to records if there is a basis for the refusal under other legislation, which could include:

- Records contain information about another person(s)
- Medical/psychiatric records (other than if supplied by you or an employer)
- Information provided by third parties such as evaluative opinion material obtained confidentially in the course of performing reference checks
- That giving access would pose a serious threat to the life, health or safety of any individual
- The request is deemed frivolous or vexatious
- The information relates to legal proceedings
- Giving access would be unlawful.



If individuals find that personal information that DPS holds is inaccurate, out of date, incomplete, irrelevant or misleading, they can ask DPS to correct the information. DPS will take such steps as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

If DPS has disclosed personal information that is inaccurate, out of date, incomplete, irrelevant or misleading, the affected individual can ask DPS to notify the third parties to whom the disclosure was made and DPS will take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

4.5 Use

DPS is committed to taking reasonable steps to ensure that the personal information held will only be used for the purpose for which it was collected.

DPS will take steps to protect personal information from:

- misuse, interference and loss; and
- unauthorised access, modification or disclosure.

4.6 Disclosure to relevant authorities

DPS reserves the right to make disclosures to relevant authorities where the use of personal information raises a suspicion that an offence is being, or has been, committed. This disclosure of such information will be consistent with any protocols, agreements and other binding arrangements in force within the parliament

DPS will disclose more extensive information than stated above in the following circumstances:

- unauthorised attempts to access files that are not published NSW Parliament websites;
- unauthorised tampering or interference with files published on the NSW Parliament websites or systems;
- unauthorised attempts to index the contents of the NSW Parliament sites by other sites or systems;
- attempts to intercept messages of other users of the NSW Parliament sites and systems;
- communications which are defamatory, abusive, vilify individuals or groups or which give rise to a suspicion that an offence is being committed;
- attempts to otherwise compromise the security of Parliament of NSW computer systems, web servers, breach the laws of the state of New South Wales or



Commonwealth of Australia, or interfere with the enjoyment of the NSW Parliament websites by other users.

In the event of an external investigation by any law enforcement agency (e.g. NSW Police, or ICAC or the AFP) that may exercise a warrant, DPS will comply with such lawful orders and provide access to all relevant systems, audit logs and data as required.

5.0 Grievance mechanisms/sanctions

Privacy related enquiries or complaints regarding our compliance with the *Privacy and Personal Information Protection Act 1998* (PIIP Act) should be made in writing using the [form](#) provided by the Information and Privacy Commissioner and directed to:

Chief Executive
Parliamentary Services
Parliament House, Macquarie St Sydney NSW, 2000
Email: DPS.ExecutiveOffice@parliament.nsw.gov.au

Your enquiry or complaint will be responded to within 14 days.

If you are not happy with the outcome of your complaint you may complain to an investigative agency such as the NSW Privacy Commissioner (www.ipc.nsw.gov.au). For more information on the process please see <https://www.ipc.nsw.gov.au/privacy/citizens/make-complaint>

6.0 Accountabilities

The Chief Executive, Parliamentary Services is responsible for approving and assuring compliance with this policy.

All DPS staff are responsible for complying with the DPS Privacy Policy, and the policies and guidelines for accessing and using DPS systems, including IT systems, and understanding their responsibilities under the PPIIP Act and the Information Protection Principles. IPC NSW e-learning modules are available.

7.0 Related policies, legislation, guidelines and forms

7.1 Legislation

- *Privacy and Personal Information Protection Act 1998*
- *Health Records Information Privacy Act 2002*



7.2 Policies and supporting documents

- Closed Circuit Television (CCTV) and Security Access Control Systems (NSW Parliament House) Policy
- Parliament House Security Pass Policy
- Public Interest Disclosures Policy (DPS)
- Records Management Policy
- IT Access and Use Policy
- IT Operations Policy
- Data Backup, Restoration, Storage and Retention Standard
- Monitoring and Event Management Procedure
- Cyber Security Policy
- Access Management Standard
- Applications Security Standard

7.3 Forms

- Privacy Complaint Internal Review Application Form
<https://www.ipc.nsw.gov.au/privacy/citizens/make-complaint-forms>

8.0 Policy review

This policy must be reviewed once each Parliament, or as required in response to changes in legislation and/or regulation.

9.0 Further information

Further information is available from the website of the [Information and Privacy Commission New South Wales](#).

10.0 Document control

Version No.	Date of issue	Record No.	Description of change/approval reference	Author
1.0	12 October 2022	POL2022/04	New policy, approval ref D22/35653.	Manager, Records & Archives, Executive Director Parliamentary Services and Executive Director Corporate Services