Greater Sydney Commission

PRIVACY MANAGEMENT PLAN

DECEMBER 2020

Document management

Approved	Danielle Smalley - Chief Operating Officer Finance and Governance Committee
Author	Mouna Kheir - Senior Projects Advisor Rachael Lemon – Manager Government Services
Revision history	Version 1 - July 2019; Version 2 – December 2020
Revision date	December 2020 – Approved by Phil Skidmore
Next review date	December 2022
Responsible branch	Operations and Governance

Contents

PART ONE – PRIVACY MANAGEMENT PLAN

1. About this Privacy Management Plan

The Greater Sydney Commission (the Commission) takes the privacy of its staff and stakeholders seriously and will manage and protect personal information with the use of this Plan as a reference and guidance tool.

The purpose of this Privacy Management Plan (the Plan) is to:

- demonstrate to members of the public how the Commission respects the privacy of our stakeholders, staff and others who we hold personal information about;
- detail the Commission's commitment to protecting the privacy of its stakeholders and staff about whom the Commission holds personal or health information;
- act as a reference tool for staff of the Commission, to explain how to best meet our privacy obligations under the *Privacy and Personal Information Protection Act 1998* (PPIPA) and the *Health Records and Information Privacy Act 2002* (HRIPA);
- inform staff about how to manage and protect personal and health information;
- describe how people can request access to and/or amendment of their personal or health information, held by the Commission;
- integrate the information protection principles and health privacy principles into existing and future policies, guidelines and procedures that address information issues;
- set complaint handling and internal review procedures;
- inform people about how to request an internal review; and
- explain the right for people to apply to the NSW Civil and Administrative Tribunal, in cases where they remain dissatisfied with internal review findings.

2. Privacy management legislation

The PPIPA and HRIPA contain principles on how to collect, store, access, amend, use and disclose personal and health information.

The PPIPA covers personal information other than health information and requires the Commission to comply with 12 information protection principles (IPPs). The IPPs cover the full 'life cycle' of information, from collection through to disposal. They include obligations about data security, quality (accuracy) and rights of access and amendment to one's own information, as well as how personal information may be collected, used and disclosed.

Health information is regulated by slightly different principles. There are 15 health privacy principles (HPPs) in the HRIPA with which the Commission must also comply. It includes information about a person's disability and health/disability services provided to them.

There are exemptions to many of the privacy principles in the two Acts themselves, and in Regulations, Privacy Codes and Public Interest Directions.

Warning

It is a criminal offence, punishable by up to two years' imprisonment, for any staff member (or former staff member) of the Commission to intentionally use or disclose any personal information about another person, to which the staff member has or had access in the exercise of his or her official functions, except as necessary for the lawful exercise of his or her official functions.

3. Who does this Plan apply to?

The Privacy Management Plan applies to Commission members (Commissioners), Youth Panel members and all employees including:

- permanent;
- temporary;
- casual staff; and
- other Government sector employees on secondment or assigned to the Commission;
- contractors, consultants and volunteers; and
- employees of organisations who provide services under contract to the Commission.

For the purposes of this Plan, “staff” refers to all people to whom this Plan applies.

In this Plan, a reference to a senior executive manager means:

- Chief Executive Officer;
- Executive Director; and
- Director.

4. Key responsibilities

Chief Executive Officer (CEO)

The CEO is responsible for ensuring that the Commission establishes and maintains systems and processes for privacy management in compliance with the PPIPA and HRIPA.

Senior executive managers and managers

A senior executive manager or a manager responsible for supervising or managing an individual or group of staff, is responsible for:

- making staff aware of this Plan and providing guidance on how to apply it;
- ensuring staff are provided with access to privacy training;
- identifying privacy issues when implementing new systems; and
- assisting staff to manage privacy issues.

All Staff

All staff are required to comply with the PPIPA and HRIPA. This Plan is intended to assist staff to understand and comply with their obligations under those Acts. If Commission staff feel uncertain as to whether certain conduct may breach their privacy obligations, they should seek the advice of the Privacy Officer.

Privacy Officer

The Privacy Officer is responsible for:

- ensuring the Privacy Management Plan is up to date and publicly available;
- ongoing training and education of Commission staff in relation to privacy;
- reporting on privacy issues in the Commission's annual report including a statement of compliance with requirements of the PPIPA and HRIPA and statistical details of any internal reviews conducted by or on behalf of the Commission;
- advising and assisting staff and the public in responding to requests for information;
- being the point of contact for staff and stakeholders relating to privacy matters;
- monitoring the effectiveness of the plan and proposing refinements where appropriate including:
    - the introduction of a significant new collection of personal information; or
    - if any new or modification of a code or direction of the Privacy Commissioner significantly changes the application of the IPPs to the Commission's operations; or
    - every two years, or earlier if required.

When amended, a copy of the amended Plan should be circulated to all Commission staff and the NSW Privacy Commissioner as soon as possible after each amendment.

5. Definitions

Collection of personal information	means the way the Commission acquires the information and can be by any means, including a written form, a verbal conversation, an online form, or taking a picture with a camera.
Disclosure	means when the Commission provides personal information to an individual or body outside the Commission.
Exemptions	means exemptions from compliance with the privacy principles both within the privacy principles and under Part 2 of the PPIPA.
Health information	See section 6.
Holding personal information	the Commission will be considered to be 'holding' personal information if it is in the Commission's possession or control, or if it is held by a contractor or service provider on our behalf. For example, information about staff in the physical possession of GovConnect is considered to be 'held' by the Commission, and the Commission remains responsible for how it is handled.
Personal information	See section 6.
Privacy obligations	means the privacy principles and any exemptions to those principles that apply to the Commission.
Sensitive personal information	means personal information that is also about a person's race, ethnicity, religion, sexuality, political or philosophical beliefs or membership of a trade union

6. Types of personal and health information held

6.1 Personal information

Personal information is defined in section 4 of the PPIPA as:

- 'information or an opinion about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion'.

Personal information is information that identifies a person and could be:

- a written record which may include their name, address and other details; or
- electronic records, photographs, images, video or audio footage and maps; or
- biometric information such as fingerprints, blood, and records of genetic material.

The PPIPA excludes certain types of information. The most significant exemptions are:

- information contained in publicly available publications;
- information about a person's suitability for public sector employment;
- information about people who have been deceased for more than 30 years;
- a number of exemptions relating to law enforcement investigations;
- matters arising out of a Royal Commission or Special Commission of Inquiry;
- matters contained in Cabinet documents;
- information exchanged between public sector agencies in certain circumstances;
- information disclosed to another public sector agency under the administration of the same Minister or under the administration of the Premier.

6.2 Health information

Section 6 of the HRIPA defines 'health information' as:

i) personal information or an opinion about:

- the physical or mental health or disability (at any time) of an individual;
- an individual's express wishes about the future provision of health services to him or her;
- a health service provided, or to be provided, to an individual,

or

ii) other personal information collected

- relating to provision of a health service;
- in connection with the donation of an individual's body parts, organs or body substances;
- about genetic information pertaining to an individual arising from health service provisions that could potentially predict the health of the individual or his/her relative.

This Plan refers to 'personal information', which in all applicable instances includes health information, unless otherwise specified.

6.3 Types of Personal Information held

The types of personal information held by the Commission include:

- Contact details and personal information relating to:
  - Greater Sydney Commissioners and Youth Panel members;
  - Government Ministers and their staff, government agency heads and senior executives, members of intra-governmental and inter-governmental committees, members of boards and advisory committees;
  - stakeholders and members of the public making submissions and participating in Commission events and requests for feedback;
  - staff in other government agencies;
  - volunteers, third parties and contractors engaged by the Commission;
  - people who submit complaints to the Commission;
- Personal information of applicants under the *Government Information (Public Access Act 2009* (GIPA Act);
- Records relating to dealing with lobbyists and business contacts;
- Staff and personnel records in the form of:
  - payroll, attendance and leave records;
  - training, disciplinary, performance management and evaluation records;
  - conflict of interest and private interest declarations;
  - workers compensation records and work health and safety records;
  - records of gender, ethnicity and disability of staff for equal employment opportunity reporting purposes.

7. Accessing or amending information

People can ask the Commission for access to and/or amendment of the personal information it holds about them. Applications or queries should be directed to the Privacy Officer.

8. Privacy complaints and internal reviews

Any person may make a privacy complaint, by applying for an ‘internal review’ of the conduct they believe breaches an IPP and/or a HPP.

Internal review is the process by which the Commission manages formal, written privacy complaints about how it has dealt with personal information. All written complaints about privacy are considered to be an application for internal review, even if the applicant does not use the words ‘internal review’.

By law, an application for internal review must:

- be in writing and addressed to the Commission;
- specify an address in Australia to which the applicant is to be notified after the completion of the review; and
- be lodged at the Commission within six months from the time the applicant first became aware of the conduct that they want reviewed.

The Commission encourages the use of the Internal Review Application Form.

An application for internal review can be made on behalf of someone else.

Where the applicant is not literate in either English and where there is no other organisation making the application on their behalf, staff should help the person to write their application.

Staff should use a professional interpreter, if necessary. Applications in other languages will be accepted and translated, and all acknowledgments and correspondence to the applicant will be translated.

Applications for internal review, or any written complaint about privacy, received at the Commission's office should be forwarded immediately to the Commission's Privacy Officer.

If the complaint is about an alleged breach of the IPPs and/or HPPs, the internal review will be conducted by the Privacy Officer, or by another person appointed by the CEO who:

- was not involved in the conduct which is the subject of the complaint;
- is an employee or an officer of the agency; and
- is qualified to deal with the subject matter of the complaint.

8.1 Extensions of time for lodgement

While the PPIP Act allows applicants six months to apply for an internal review from the time the applicant first becomes aware of the conduct, the Commission may accept late applications. Possible acceptable reasons for delay may be:

- the applicant's ill-health or other reasons relating to capacity; or
- the applicant only recently becoming aware of their right to seek an internal review: or
- the applicant reasonably believing that they would suffer ill-effects as a result of making an application for internal review.

However, late applications that, because of their age, cannot be investigated in a meaningful way will be declined. In these cases, witnesses may no longer be available, documents may have been destroyed and corporate memory may be an issue.

Final decisions on the acceptance of late applications will only be made by the Commission's CEO or Chief Operating Officer. Where the decision is made not to accept an application because it is too old, the reason will be explained in a letter to the applicant.

8.2 The Internal Review process

When the Commission receives an internal review application, the Privacy Officer will:

- send an acknowledgment letter to the applicant and advise that if the internal review is not completed within 60 days they have a right to seek a review of the conduct by the NSW Civil and Administrative Tribunal; and
- send a letter to the NSW Privacy Commissioner with details of the application. A copy of the written complaint will also be provided to the Privacy Commissioner.

Internal reviews follow the process set out in the Information and Privacy Commission NSW's Internal Review Checklist. When the internal review is completed, the Commission's Privacy Officer will notify the applicant in writing of:

- the findings of the review;
- the reasons for the finding, described in terms of the IPPs and/or HPPs;
- any action the Commission proposes to take and the reasons for the proposed action (or no action); and
- the applicant's entitlement to have the findings and the reasons for the findings reviewed by the NSW Civil and Administrative Tribunal.

The Commission will also send a copy of that letter to the NSW Privacy Commissioner.

Statistical information about the number of internal reviews conducted must be maintained for the Commission's Annual Report.

8.3 External Review by the NSW Civil and Administrative Tribunal

People may apply to the Tribunal for an external review of the conduct which was the subject of their earlier internal review application. The Tribunal may make orders requiring the Commission to:

- refrain from conduct or action which breaches an IPP, HPP or Code
- perform in compliance with an IPP, HPP or Code;
- correct information disclosed by the Commission; or
- take steps to remedy loss or damage.

The Tribunal may also make an order requiring the Commission to pay damages of up to $40,000 if the applicant has suffered financial loss or psychological or physical harm as a result of the conduct.

9. Privacy Impact Assessment

A Privacy Impact Assessment (PIA) may be required to assess any actual or potential effects that an activity may have on personal information held by the Commission. A PIA can also outline mitigation strategies for any identified risks and any positive impacts enhanced.

Public consultation and measuring community expectation is an important part of any thorough PIA. A PIA should examine both the positive (privacy-enhancing) and negative (privacy-invasive) impacts, but primarily focus on the negative impacts and their mitigation.

Privacy risks can be avoided or mitigated by:

- ensuring a project complies with the law or meets community expectations;
- making a project less privacy-invasive; and
- making a project more privacy-enhancing.

It may not be possible to eliminate every risk, but a judgement will be made as to whether the public benefit to be derived from the project will outweigh the risk posed to privacy.

To know if a PIA is required, staff should refer to Appendix A, which sets out a PIA checklist. If the answer to one of more of those questions is "yes", then advice should be sought from the Privacy Officer and a PIA should be considered. There are many benefits in carrying out a PIA, such as it:

- helps to ensure compliance with privacy legislation;
- helps reduce costs later in management time, legal expenses and potential media or public concern by considering privacy issues early;
- assists in anticipating and responding to the public's possible privacy concerns;
- enhances informed decisions-making at the right level; and
- enhances the legitimacy of a project, especially where some compromise or trade-off is necessary.

A PIA will diagnose what risks, benefits, costs and safeguards are involved.

10. Further information and resources

Internal Policies

- Greater Sydney Commission Code of Ethics and Conduct

- Greater Sydney Commission Grievance Resolution Policy
- Greater Sydney Commission Work, Health and Safety Policy
- Greater Sydney Commission Managing Unsatisfactory Performance Procedure
- Greater Sydney Commission Conflict of Interest

Legislation

- *Privacy and Personal Information Protection Act 1998 (NSW)*
- *Health Records & Information Privacy Act 2002 (NSW)*
- *Anti-Discrimination Act 1977*
- *Criminal Records Act 1991*
- *Government Information (Public Access) Act 2009*
- *Ombudsman Act 1974*
- *Public Interest Disclosures Act 1994*
- *State Records Act 1998*
- *Workplace Surveillance Act 2005*

Other resources

Information and Privacy Commission NSW – www.ipc.nsw.gov.au

PART TWO – PRIVACY PRINCIPLES

Important note about using this part of the Plan

This part of the Plan uses plain language, not the exact wording of the law. This is to make understanding the Commission's obligations easier. This document does not cover the full complexity of the privacy laws applying to the Commission. It has been simplified and does not cover all exemptions or situations.

If in doubt, the exact wording in the legislation should be checked, and guidance sought from the Commission's Privacy Officer, or the NSW Privacy Commissioner.

This document is an educational tool, not legal advice.

1. How the privacy principles apply

The privacy principles are the standards which the Commission is expected to follow when dealing with personal information and health information.

The phrase 'privacy principles' refers to the combination of the 12 information protection principles (IPPs) set out in Division 1 of the PPIPA, and the 15 health privacy principles (HPPs) in Schedule 1 of the HRIPA.

There are a number of ways that the Commission's conduct may be exempt from one or more of the IPPs or HPPs. Exemptions are found in the PPIPA and HRIPA, in written directions made by the Privacy Commissioner, and in Privacy Codes of Practice. In some cases, other legislation will override the privacy principles.

The following section uses plain language (not the wording of the law itself) to describe the privacy principles and how Commission staff must comply with them. It also mentions the exemptions that may be relevant for the Commission, depending on the context. The Commission's Privacy Officer can provide guidance on interpreting the requirements of the privacy principles or exemptions.

1.1. Introduction to the application of the privacy principles

The Commission's privacy obligations have been condensed into the following 13 plain language principles:

1. limiting our collection of personal information;
2. anonymity;
3. unique identifiers;
4. how we collect personal information – the source;
5. how we collect personal information – the method and content;
6. notification when collecting personal information;
7. security safeguards;
8. transparency;
9. access;
10. correction;
11. accuracy;
12. use; and
13. disclosure.

2. Condensed Principles

This section of the plan summarises the 13 condensed principles.

2.1. Limiting the collection of personal information

The principle in brief

The Commission will only collect personal information if:

- it is for a lawful purpose that is directly related to the Commission's functions; and
- it is reasonably necessary for the Commission to have the information.

Key messages, examples and definitions

The Commission will not ask for personal information unless it is needed. The Commission will especially avoid collecting sensitive personal information if it is not required.

By limiting the collection of personal information to only what the Commission needs, it is easier to comply with privacy obligations.

⇒ Example: when designing a form, ask: "do we require each piece of this information?"

Common exemptions

Relevant exemptions include:

- unsolicited information;
- information collected before 1 July 2000.

Before relying on an exemption, staff must check with the Commission's Privacy Officer.

⇒ For example: the 'unsolicited' exemption from the rules for collection of personal information may not apply if the Commission has invited a person to provide personal information, such as through a complaints process.

2.2. Anonymity

The principle in brief

The Commission will allow people to receive services anonymously, where lawful and practicable.

Key messages, examples and definitions

⇒ For example: People making informal enquiries are provided with information about the Commission's activities, without having to identify themselves.

Common exemptions

None.

2.3. Unique identifiers

The principle in brief

The Commission will allow people to receive services anonymously, where lawful and practicable.

The Commission does not assign identifiers to people who receive services. The Commission avoids collecting unique identifiers (other than tax file numbers from staff).

Key messages, examples and definitions

Identifiers can assist with efficient record management, but they also pose privacy risks if they are used to match or compile large quantities of data about a person from different sources. For that reason, sharing unique personal identifiers between different organisations is generally prohibited.

A unique personal identifier is not just a person's name or file number. It can be a key (such as a number) which aims to uniquely identify a person. A tax file number, Centrelink ID or a driver's licence number is a unique personal identifier.

⇒ For example, so that the Commission can separate all the different people with the name 'John Smith'.

The Commission avoids collecting unique personal identifiers, although the Commission does collect tax file numbers of staff, from staff members themselves.

Common exemptions

None.

2.4. How the Commission collects personal information – the source

The principle in brief

The Commission collects personal information directly from the person unless either they have authorised otherwise or, in the case of health information, it would be unreasonable or impractical to obtain the personal information directly from the person.

Staff records are administered in accordance with the Public Sector Personnel Handbook which is available at www.psc.nsw.gov.au.

Key messages, examples and definitions

If the Commission needs information about Sue, staff should ask Sue herself, rather than Jim. By collecting information direct from the source, it will be easier for the Commission to comply with other obligations, like ensuring the accuracy of the information, and getting permission for any disclosures of the information.

However, there may be circumstances where it is not possible to collect the information directly from the person:

- For example: A person attending a Commission public event has fainted, and a staff member has called the first aid officer. It is okay to ask the person's friend for some health information about them ("do you know if they are diabetic?") because it is unreasonable and impractical to ask the person directly.

Common exemptions

Common exemptions include:

- unsolicited information;
- where the person is under 16, the information can be collected from their parent or guardian (but this is not compulsory);
- if another law authorises or requires collection of the information indirectly (i.e. from a different source);

- for some law enforcement and investigation purposes, information collected before 1 July 2000;
- if compliance would, in the circumstances, prejudice the interests of the individual to whom the information relates.

Before relying on an exemption, staff must check with the Commission's Privacy Officer.

Other relevant points

Where a person lacks some capacity (e.g. because of a brain injury), the Commission can ask their authorised representative for the information instead, however the Commission must also still try to communicate with the person directly. The Information and Privacy Commission NSW's document, Guide: Privacy and people with decision making disabilities explains how to collect personal information from or about a person who has limited or no capacity.

The Office of the Privacy Commissioner NSW's Handbook to Health Privacy provides some other examples of when it might be "unreasonable or impractical" to collect health information directly from the person.

2.5. How the Commission collects personal information – method and content

The principle in brief

The Commission:

- will not collect personal information by unlawful means;
- will not collect personal information that is intrusive or excessive;
- will ensure that the personal information we collect is relevant, accurate, up-to-date, complete, and not misleading.

Key messages, examples and definitions

The Commission will not ask for information that is not relevant or sensitive personal information; however, only 'reasonable steps' need to be taken to meet this standard.

To determine what might be 'reasonable steps', the Commission will consider:

- the sensitivity of the information;
- the possible uses of the information; and
- the practicality and cost of aiming for 'best practice'.

For Example: The Commission wants to do a client satisfaction survey of people who attended community consultation sessions. It is not relevant for the Commission to know each participant's home address, date of birth or marital status.

Common exemptions

Common exemptions include:

- unsolicited information
- information collected before 1 July 2000.

Before relying on an exemption, staff must check with the Commission's Privacy Officer.

2.6. Notification when collecting personal information

The principle in brief

When collecting personal information, the Commission will take reasonable steps to tell the person:

- who will hold and/or have access to their personal information;
- what it will be used for;
- what other organisations (if any) routinely receive this type of personal information from the Commission;
- whether the collection is required by law;
- what the consequences will be for the person if they do not provide the information to the Commission; and
- how the person can access their personal information held by the Commission.

Special rule for health information

As a general rule, the Commission must ensure robust notification systems when collecting health information more so than when collecting other types of personal information given the sensitivity of this information.

Key messages, examples and definitions

Individuals providing their personal information to the Commission have a right to know the full extent of how the information they provide will be used and disclosed, and to choose whether or not they wish to go ahead with providing information on that basis. Notification is done through a 'privacy notice'.

Privacy notices can be given in writing or verbally, but written notice is preferable. The Commission needs to take reasonable steps to ensure each relevant person receives the notice. To determine what might be "reasonable steps", we will consider:

- the sensitivity of the information;
- the possible uses of the information; and
- the practicality and cost of aiming for 'best practice'.

Where the person lacks some capacity (e.g. because of a brain injury), the Commission must notify their authorised representative, but also still try to communicate with the person directly.

Common exemptions

Common exemptions include:

- unsolicited information;
- information collected before 1 July 2000;
- if another law authorises or requires the Commission to not notify people for some law enforcement and investigation purposes;
- the person has already been notified by the organisation that gave the Commission the information.

Before relying an exemption, staff must check with the Commission's Privacy Officer.

Other relevant points

When drafting a privacy notice, staff should use the template privacy notice attached in Appendix B to this document. Any new projects which might collect personal information

should be reviewed by the Commission's Privacy Officer to ensure an adequate privacy notice is included.

The Information and Privacy Commission NSW's document, Guide: Privacy and people with decision making disabilities explains how to notify a person who has limited capacity to understand.

2.7. Security safeguards

The principle in brief

The Commission will:

- take reasonable security measures to protect personal information from loss, unauthorised access, use, modification or disclosure;
- ensure personal information is stored securely, not kept longer than necessary, and disposed of appropriately.

Special rule for health information

As a general rule, the Commission must work harder to protect health information (or any sensitive personal information that may be held).

Key messages, examples and definitions

The Commission must take reasonable steps to ensure it secures all information it holds. Security measures could include technical, physical or administrative actions.

⇒ For example: personal information must be provided to a contractor or service provider only if they really need it to do their job. Reasonable steps must be taken by the Commission to prevent any unauthorised use or disclosure of the information by a contractor or service provider, and contractors are obligated to comply with the same privacy obligations as the Commission.

⇒ Sensitive personal information (if held by the Commission) will not be disclosed without the person's express consent.

⇒ For example: The Commission must follow good practice records management in relation to saving and adequately securing information.

To determine what might be "reasonable steps", the Commission will consider:

- the sensitivity of the information;
- the context in which the information was obtained;
- the purpose for which the Commission collected the information;
- the possible uses of the information; and
- the practicality and cost of aiming for 'best practice'.

Common exemptions

None.

2.8. Transparency

The principle in brief

The Commission will enable anyone to know:

- whether the Commission is likely to hold their personal information;
- the purposes for which the Commission uses personal information; and
- how they can access their own personal information.

Key messages, examples and definitions

The Commission has a broad obligation to the community, to be open about how it handles personal information. This is different to collection notification, which is much more specific, and given at the time of collecting new personal information.

⇒ For example: This Plan will be available on our website. This Plan briefly explains our privacy obligations and sets out how we will handle the major categories of personal and health information that we hold.

Common exemptions

None.

2.9. Access

The principle in brief

The Commission will:

- allow people to access their personal information without unreasonable delay or unreasonable expense;
- only refuse access where authorised by law, and will provide written reasons for the refusal, if requested.

Key messages, examples and definitions

People should generally be able to see what information the Commission holds about them, with minimal barriers. The Commission's policy is that as much as possible, it will let complainants, clients and staff see their own personal information at no cost, and through an informal request process.

The Commission cannot charge people to lodge a request for access, but reasonable fees can be charged for copying or inspection, if the Commission tells people what the fees are up-front. Fees should be no more than for the fees charged for access under the GIPA Act. Under the GIPA Act, the Commission can charge up to $30 per hour for the work it takes to identify the information sought and consider whether it may be released.

If there is personal information about other individuals or confidential information about third parties in any records identified by our searches, then the Commission's GIPA officer (info@gsc.nsw.gov.au) will process the request for access, rather than the area that holds the record. This will ensure that the privacy and confidentiality of other people and third parties can also be properly considered.

Common exemptions

A common exemption is:

- in some circumstances another law may prevent the Commission from giving the person access to the information requested.

Before relying on an exemption, staff must check with the Commission's Privacy Officer.

Other relevant points

Any unusual request to access personal information should be put in writing, and then referred to the Commission's Privacy Officer to review.

The Information and Privacy Commission NSW's document, Guide: Privacy and people with decision making disabilities explains how to provide access to personal information held about a person who has limited or no capacity.

Formal access applications under the GIPA Act will be handled by the Commission's GIPA officer (info@gsc.nsw.gov.au).

2.10. Correction

The principle in brief

The Commission will allow people to update or amend their personal information, to ensure it is accurate, relevant, up-to-date, complete or not misleading.

Where possible, the Commission will notify any other recipients of any changes.

Key messages, examples and definitions

If the Commission disagrees with the person about whether the information needs changing, it must instead allow the person to add a statement to the Commission's records.
The Commission cannot charge people to lodge a request for access, but reasonable fees can be charged for copying or inspection, if the Commission tells people what the fees are up-front. Fees should be no more than for the fees charged for access under the GIPA Act. Under the GIPA Act, the Commission can charge up to $30 per hour for the work it takes to identify the information sought and consider whether it may be released.

The Commission's policy is that as much as possible, it will let complainants, clients and staff update their own personal information at no cost, and through an informal request process. This does not mean they can just ask us to alter their personnel file without going through the proper processes.

For Example: When a stakeholder or member of the public calls to notify a change in their mailing address, we will update their contact details quickly and for no cost.

Common exemptions

A common exemption is:

- if another law authorises or requires us to not to amend the information

Before relying on an exemption, staff must check with the Commission's Privacy Officer

Other relevant points

Any unusual request to amend personal information should be put in writing, and then referred to the Commission's Privacy Officer to review.

2.11. Accuracy

The principle in brief

Before using or disclosing personal information, the Commission will take appropriate steps to ensure that the information is relevant, accurate, up-to-date, complete, and not misleading.

Key messages, examples and definitions

The Commission must ensure that personal information is still relevant and accurate before it is used or disclosed.

The Commission only needs to take reasonable steps to check the information – but more steps will be needed if the information is likely to be used in a way that will disadvantage the person.

What might be considered “reasonable steps” will depend upon the circumstances, but some points to consider are:

- the context in which the information was obtained;
- the purpose for which the Commission collected the information;
- the purpose for which the Commission now wants to use the information;
- the sensitivity of the information;
- the number of people who will have access to the information;
- the potential effects for the person if the information is inaccurate or irrelevant;
- any opportunities the Commission has already given the person to correct inaccuracies; and
- the effort and cost involved in checking the information.

⇒ For Example: When the Commission is investigating a workplace grievance, it will give the person who is the subject of the complaint an opportunity to correct the information being relied on before making a final decision.

Common exemptions

Common exemptions include:

- to deal with a serious and imminent threat to any person;
- if another law authorises or requires us to use the information;
- some law enforcement and investigative purposes.

Before relying on an exemption, staff must check with the Commission’s Privacy Officer.

2.12. Use

The principle in brief

The Commission may use personal information:

- for the primary purpose for which it was collected;
- for a directly related secondary purpose within the reasonable expectations of the person; or
- for another purpose if the person has consented.

Key messages, examples and definitions

The Commission should only use personal information for the purpose for which it was collected. It should not seek new uses for people’s personal information.

For example: If the primary purpose of collecting a complainant's information was to investigate their workplace grievance, a directly related secondary purpose within the reasonable expectations of the person for which their personal information could be used by the Commission, would include independent auditing of workplace grievance files.

Common exemptions

- Common exemptions include:
    - to deal with a serious and imminent threat to any person;
    - if another law authorises or requires the Commission to use the information;
    - some law enforcement and investigative purposes.

Before relying on an exemption, staff must check with the Commission’s Privacy Officer

Other relevant points

The primary purpose for which the Commission collected the information should have been set out in a privacy notice. To use personal information for a purpose set out in the privacy notice is acceptable, but for any other purpose, staff must check with the Commission's Privacy Officer first.

The Information and Privacy Commission NSW's document, Guide: Privacy and people with decision making disabilities, explains how to seek consent for a secondary use of personal information from a person who has limited or no capacity.

The Office of the Privacy Commissioner NSW's Statutory Guidelines on Research explain how health information can be used for research purposes. It also provides a good rule of thumb for the use of other types of personal information for research purposes.

2.13. Disclosure

The principle in brief

The Commission will only disclose personal information if:

- at the time the Commission collected their information the person was given a privacy notice to inform them their personal information would or might be disclosed to the proposed recipient; or
- the disclosure is directly related to the purpose for which the information was collected, and the Commission has no reason to believe that the individual concerned would object to the disclosure; or
- the person concerned has consented to the proposed disclosure.

Special rule for health information

Tougher rules also apply when transferring health information outside of NSW (including to the Commonwealth Government). The Commission can only transfer health information outside NSW if one of the following applies:

- the person concerned has consented;
- if it is necessary for a contract with (or in the interests of) the person concerned;
- if it will benefit the person concerned, the Commission cannot obtain their consent, but believes the person would be likely to give their consent;
- the Commission reasonably believes that the recipient of the information is subject to a law or binding scheme equivalent to the HPPs; or
- the Commission has bound the recipient by contract to privacy obligations equivalent to the HPPs.

Key messages, examples and definitions

The Commission can usually disclose information in ways clearly notified to the person at the time their personal information was collected. However, if the Commission did not tell the person about the proposed disclosure in a privacy notice, or if it is health information and the Commission wants to send it outside NSW, it is usually necessary to get the person's consent for the disclosure.

In addition:

- section 27A of the PPIPA provides that the Commission is not required to comply with the privacy principles in relation to the collection, use or disclosure of personal information if:

(a) the Commission is providing the information to another public sector agency or the Commission is being provided with the information by another public sector agency, and

(b) the collection, use or disclosure of the information is reasonably necessary:

(i) to allow any of the agencies concerned to deal with, or respond to, correspondence from a Minister or member of Parliament, or

(ii) to enable inquiries to be referred between the agencies concerned, or

(iii) to enable the auditing of the accounts or performance of a public sector agency or group of public sector agencies (or a program administered by an agency or group of agencies).

- section 28 (3) of the PPIPA provides that information may be disclosed:

(a) by a public sector agency to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or

(b) by a public sector agency to any public sector agency under the administration of the Premier if the disclosure is for the purposes of informing the Premier about any matter.

Common exemptions

Common exemptions include:

- under sections 27A and 28 (3) of the PPIPA Act;
- information about a person's suitability for public sector employment;
- to deal with a serious and imminent threat to any person;
- to deal with a serious threat to public health or safety (health information only);
- if another law authorises or requires us to disclose the information;
- if a subpoena, warrant or 'notice to produce' requires us by law to disclose the information for some law enforcement and investigative purposes.

Before relying on an exemption, staff must check with the Commission's Privacy Officer.

Other relevant points

The primary purpose for which the Commission collected the information should have been set out in a privacy notice. To disclose personal information for a purpose set out in the privacy notice is acceptable, but for any other purpose, check with the Commission's Privacy Officer first.

The Information and Privacy Commission NSW's document, Guide: Privacy and people with decision making disabilities explains how to seek consent for a disclosure of personal information from a person who has limited or no capacity.

The Office of the Privacy Commissioner NSW's Statutory Guidelines on Research explain how health information can be disclosed for research purposes. It also provides a guideline for the disclosure of other types of personal information for research purposes.

Appendix A: Privacy Impact Assessment checklist

If the answer to one or more of the questions below is yes, then a Privacy Impact Assessment should be considered.

A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating that impact.

Will the project involve?		Yes	No
1	The collection of personal information, compulsorily or otherwise?		
2	A new use of personal information that is already held?		
3	A new or changed system of regular disclosure of personal information, whether to another agency, another State, the private sector, or to the public at large?		
4	Restricting access by individuals to their own personal information?		
5	New or changed confidentiality provisions relating to personal information?		
6	A new or amended requirement to store, secure or retain particular personal information?		
7	A new requirement to sight, collect or use existing ID, such as an individual's driver's licence?		
8	The creation of a new identification system, e.g. using a number, or a biometric?		
9	Linking or matching personal information across or within agencies?		
10	Exchanging or transferring personal information outside NSW?		
11	Handling personal information for research or statistics, de-identified or otherwise?		
12	Powers of entry, search or seize, or other reasons to touch another individual (e.g. taking a blood or saliva sample)?		
13	Surveillance, tracking or monitoring of individuals' movements, behaviour or communications?		
14	Moving or altering premises which include private spaces?		
15	Any other measures that may affect privacy?		

If the above shows a need to carry out a Privacy Impact Assessment, contact the Privacy Officer.

If a PIA is not needed, make a note and copy of the above questions and save to file. This helps if privacy issues arise later in the project and you need to re-visit the list.

Even if the list above does not indicate the need for a PIA, it may still be advisable to create a short PIA, particularly if the project will change hands several times. A consistent approach to the management of privacy in the project is crucial.

A PIA should contain some or all of the following 10 steps:

1. **Assess the necessity for a PIA** – using the above checklist.
2. **Plan the PIA** – how detailed it needs to be:
   - Will it cover one product and service or a group of products and services?
   - Identify the primary stakeholders.
   - Scope the complexity of the product and service.
   - Will there be community or media interest in the outcome?
3. **Describe the project** (briefly).
   - What are the projects overall aims?
   - Who is responsible?
   - What is the time frame?
4. **Identify the stakeholders**.
   - Who are the stakeholders?
   - Are consultations required to discuss potential risks and concerns?
5. **Map information flows**.
   - Map the data life cycle - what is collected, how, by whom and here is it going?
   - What are the security and quality processes around the data?
   - Map the data against compliance with the IPPs and HPPs and identify gaps.
6. **Privacy impact analysis and compliance check**
   - Analyse the gaps.
   - Identify the risks and where they are coming from.
   - Identify the data or compliance leakage.
7. **Privacy management – addressing risks**
   - What options will allow you to remove, minimise or mitigate any identified risks?
   - Is collection of personal data necessary?
   - Are you being transparent enough (privacy notice issued)?
8. **Formulate recommendations for future projects.**
   - Are there any changes that would achieve a more appropriate balance between the project's goals, the interests of affected individuals, and the agency's interests?
   - Are any of the privacy impacts so significant that the project should not proceed?
9. **Prepare the report – to include the following**:
   - An overall description
   - Your PIA method
   - Description of the data flows
   - Outcome of the PIA and compliance checks
   - How to mitigate and avoid future risks
   - Identification of the community's response to these risks
10. **After the PIA report**

    - Have you responded to the recommendations in the PIA report?
    - Have you engaged an independent review of these recommendations?
    - Has the PIA changed due to any changes in the project?

It is not compulsory to have a PIA, but it is recommended.

Appendix B: Template privacy notice and consent wording

About privacy notices

When collecting personal information, the Commission should tell the person:

- whether the collection is required by law;
- what the consequences will be if they do not provide the information;
- what their personal information will be used for;
- who will hold / store the information (if not the Commission)
- who else might receive the information from the Commission, and
- how they can access or update/correct their information.

The following ***Template privacy notice*** should be used when the Commission is collecting personal information in writing, and only intends to use or disclose the information for the purpose for which it is collected.

If any other secondary use or disclosure is contemplated, also use the ***Template consent wording***, below.

If personal information is being collected verbally (e.g. over the telephone), see ***Verbal collections*** below.

Template privacy notice

The Greater Sydney Commission (the Commission) is requesting this information from you so that we can … [*describe the primary purpose for which this information is being collected – e.g. process your registration for a seminar, assess your job application, investigate your complaint, etc].* We may also *… [describe any directly related purposes for which the information might be used – e.g. auditing, reporting or program evaluation*].

For the same purpose, the Commission may provide this information about you to *… [list any persons or organisations that such information is usually disclosed to, outside of the Commission – e.g. the Minister responsible for the subject of their correspondence, or a contractor or consultant].*

The Commission will not disclose your personal information to anybody else unless we are required to do so by law – for example if the information is needed in an emergency or for a law enforcement purpose.

Providing us with the requested information is not required by law. However, if you choose not to provide us with the requested information, *… [describe the main consequences for person if information is not provided – e.g. the Commission cannot process your competition entry, or the Commission cannot investigate your complaint].*

You may request access to your information at any time. o access or update your personal information, or for more information on our privacy obligations, ask to speak to our Privacy Officer.

Template consent wording

If the Commission wishes to use or disclose personal information for an unrelated secondary purpose (i.e. a purpose not directly related to the primary purpose for which the information was collected), the Commission will generally need to seek the person's consent for that secondary use or disclosure.

Consent cannot be a 'requirement' or pre-condition to a transaction. Consent is only valid if it is voluntary, informed, specific, time-limited, and given by a person with the capacity to make decisions about the handling of their personal information.

Ideally, a request for consent will be made at the time the information is collected in the first place. Therefore, where a secondary use or disclosure of personal information is anticipated at the time of collection, the following ***Template consent wording*** should be used, as an additional part of the privacy notice, inserted after the third paragraph of the ***Template privacy notice (see above)***.

With your permission, we would also like to (use / disclose) your information to …. *(describe here the intended secondary purpose – e.g. put you on our mailing list for future community events).*

☐ I consent to my personal information being (used / disclosed) for the purpose of … *(name the secondary purpose).*

Signature:

Verbal collections

When collecting personal information verbally (e.g. during telephone discussions), we can use less formal wording, so long as we explain ***how*** the person's personal information will be used, ***and to whom else*** it will likely be disclosed. If the person asks further questions about whether the information is really needed, then we can go into more depth, and we can also mention their access and amendment rights or offer to let them speak to the Commission's Privacy Officer.

However, if we need to obtain the person's verbal consent to a secondary use or disclosure, we must explain what it is we are asking, and we must ensure that they understand they are free to say 'no'. We must also make a file-note of what was said.

Appendix C: Privacy Complaint (Internal Review Application) Form

1.	Name of the agency you are complaining about: **Greater Sydney Commission**
2.	Your full name:
3.	Your postal address:
4.	If you are complaining on behalf of someone else, write their full name here: What is your relationship to this other person? (e.g. parent or lawyer) Is the other person capable of making the complaint him or herself? ☐ Yes ☐ No ☐ I'm not sure
5.	What is the specific ***conduct*** you are complaining about? *('Conduct' can include an action, a decision, or even inaction by the Commission. For example, the 'conduct' might be a decision to refuse you access to your personal information, or the action of disclosing your personal information to another person, or a failure to protect your personal information from being inappropriately accessed by someone else.)*
6.	Please tick which of the following describes your complaint: *(You can tick more than one)* ☐ collection of my personal/health information ☐ security or storage of my personal/health information ☐ refusal to let me access or find out about my own personal/health information ☐ accuracy of my personal/health information

	□ use of my personal/health information □ disclosure of my personal/health information □ other □ I'm not sure
7.	When did the conduct occur? *(Please be as specific as you can)*
8.	When did you first become aware of this conduct?
9.	**You need to lodge this application within 6 months of the date you have written at Q.8.** If more than 6 months has passed, you need to ask the Commission's Privacy Officer for special permission to lodge a late application. If you need to, write here to explain why you have taken more than 6 months to make your complaint:
10.	What effect did the conduct have on you?
11.	What effect might the conduct have on you in the future?
12.	What would you like to see the Commission do about the conduct? *(For example: an apology, a change in policies or practices, your expenses paid, damages paid to you, training for staff, etc.)*
13.	I understand that this form will be used by the Commission to process my request for an Internal Review.

	I understand that details of my application will be referred to the NSW Privacy Commissioner as required by law, and that the Privacy Commissioner will be kept advised of the progress of the review. I would prefer the Privacy Commissioner to have: ☐ a copy of this application form, or ☐ just the information provided at Q's 5 - 12.

Your signature:

Dated:

SEND THIS FORM TO:

Privacy Officer

(Phil Skidmore: Phil.Skidmore@gsc.nsw.gov.au

<u>Ensure you keep a copy for your own records too.</u>