



## Privacy

<b>Version</b>	3.0 (2020)	<b>Contact</b>	Privacy Officer
<b>Policy Owner</b>	Chief Legal Officer	<b>Approved</b>	November 2020 to have effect 1 December 2020
<b>SharePoint</b>	Legal and Legislation	<b>Due for Revision</b>	December 2023

## Definition

The Privacy Act 2020 (the Act) controls how agencies collect, use, disclose, store and give access to personal information.

Personal information is information about identifiable, living people.

## Scope and Responsibilities

This policy covers all of the Public Service Commission (the Commission), including all current employees (fixed term, full time and secondments) and contractors.

The Commission holds personal information about its employees, chief executives and developing leaders. The Commission is trusted with this information and is committed to the protection and management of this data, fulfilling its obligations under the Act.

Information can only be accessed in accordance with the “need to know” principle. Managers in relevant Commission groups, the Leadership Team (LT) and Human Resources (People Team) are responsible for maintaining and handling this information appropriately.

This policy also covers any other personal information that the Commission collects for statistical or research purposes.

**In the event of a privacy breach** – First of all... don't panic.

While the Commission is committed to meeting its obligations under the Privacy Act, we understand that sometimes mistakes happen. In the event of a privacy breach, please contact your manager and the Commission's Privacy Officer. Even if you are not sure if you have breached the Act, you should discuss the next steps with your manager and the Privacy Officer.

By communicating breaches early, it is easier to mitigate the impact. If further action is required, the Privacy Officer will mitigate the impact from the breach and record the appropriate information in the privacy breach register. By following a systematic process in accordance to their training, they will then work with you and your manager to reduce the likelihood of any further breaches occurring.

If the Commission has a privacy breach that that is a notifiable privacy breach under the Act, the Commission will notify the Office of the Privacy Commissioner and affected individuals as soon as practicable. The Privacy Officer can advise you as to which privacy breaches are notifiable.

## Responsibilities

All employees are responsible for protecting personal information entrusted to the Commission.

LT is responsible for ensuring the Commission has appropriate policies and processes to safeguard the personal information entrusted to the Commission.

LT is responsible for creating and nurturing a respectful privacy culture at the Commission.

LT is responsible for assuring the Chief Executive that each Business Unit complies with departmental policies and processes to safeguard the personal information entrusted to the Commission.

The Chief Legal Officer owns this Policy and with the Privacy Officer is responsible for monitoring the Commission's compliance with the Privacy Act and for advising LT about any risks to the Commission's ability to protect and manage the personal information it holds.

## Principles

The Commission's management and protection of personal information will be guided by the following principles:

- All personal information we hold will be managed and used in accordance with the Act
- the Commission will promote a culture in which personal information is protected and respected
- Individuals will be confident that the Commission is a trusted guardian of their personal information.

Our commitment to privacy will be shown by:

- Only collecting personal information which is necessary to undertake our functions
- Being transparent and open about what personal information is being collected
- Giving individuals the opportunity to make an informed choice about the personal information they provide, or how much personal information they provide
- Ensuring all individuals have the right to access personal information we hold about them and the right to seek correction if that information is wrong
- Establishing a clear and lawful purpose for collecting personal information, and only using and disclosing personal information in accordance with that purpose
- Taking reasonable steps to make sure that personal information is accurate before we use it
- Protecting personal information from loss, misuse, and unauthorised access
- Responding quickly and appropriately if a privacy breach occurs or is suspected.

## To achieve this, the Commission will:

- Implement best practice end-to-end privacy management processes. We will do this by:
  - Embedding privacy by design principles into service design so that privacy protection is at the forefront of any systems and business processes that contain personal information
  - Undertaking a brief privacy analysis and, if necessary, a privacy impact assessment for new business process development where personal information is involved
  - Testing and reviewing our current systems and processes to actively identify risks to privacy and apply treatments when risks are identified
  - Following the relevant protocols and guidance under the Commission's Information Strategy. In particular, the use of the Confidentiality Guidelines when releasing any statistical information that contains personal or confidential information.
- Ensure our staff are confident and knowledgeable in their approach to managing personal information. We will do this by:
  - Providing resources and training on privacy practices
  - Developing and publishing guidance on how privacy is managed at the Commission
  - Using our privacy communication strategy to focus and raise awareness of privacy with our staff
- Regularly assess the state of our privacy health. We will do this by:
  - Reviewing and refreshing our privacy programme to continually lift our performance as measured against the Government Chief Privacy Officer annual privacy self- assessment report

- Monitoring how we manage privacy requests, complaints and breach responses and implementing changes to our processes if deficiencies are identified
- Provide effective leadership on privacy across the Commission. We will do this by:
  - Empowering our departmental Privacy Officer to undertake effective monitoring and oversight of our compliance with the requirements of the Act
  - Equipping our managers with privacy skills and knowledge so they can ‘walk the talk’ on privacy
- Ensure that members of the public understand how privacy is managed at the Commission. We will do this by:
  - Publishing our privacy policy on the Commission website to ensure the public understand the Commission’s commitment to privacy
  - Ensuring that all our websites contain accurate privacy notices and information about how individuals can access information held by the Commission.

## Principles of the Privacy Act

There are thirteen principles at the heart of the Privacy Act, arranged into eight categories. These principles outline how information is collected and used, detailing people rights to gain access to that information, or to correct it.

These principles govern the collection of personal information. This includes the reasons why personal information may be collected, where it may be collected from, and how it is collected.

### Category description Principles (with links to guidance)

Category description	Principles (with links to guidance)
These principles govern the collection of personal information. This includes the reasons why personal information may be collected, where it may be collected from, and how it is collected.	Principle One: <a href="#">Purpose for Collection</a> Principle Two: <a href="#">Source of Information</a> Principle Three: <a href="#">What to tell an individual</a> Principle Four: <a href="#">Manner of collection</a>
This principle governs the way personal information is stored. It is designed to protect personal information from unauthorised use or disclosure.	Principle Five: <a href="#">Storage and Security</a>
This principle gives individuals the right to access information about themselves.	Principle Six: <a href="#">Access</a>
This principle gives individuals the right to correct information about themselves.	Principle Seven: <a href="#">Correction</a>
These principles place restrictions on how people and organisations can use or disclose personal information. These include ensuring information is accurate and up-to-date, and that it isn’t improperly disclosed.	Principles Eight: <a href="#">Accuracy</a> Principle Nine: <a href="#">Retention</a> Principle Ten: <a href="#">Use</a> Principle Eleven: <a href="#">Disclosure</a>
This principle governs how information can be shared overseas.	Principle Twelve
This final principle governs how “unique identifiers” – such as Internal Revenue Department (IRD) numbers, bank client numbers, driver’s licenses and passport numbers – can be used.	Principle Thirteen: <a href="#">Unique identifiers</a>

For more information on the Privacy Act, please refer to the [Office of the Privacy Commissioner website](#).