OFFICE OF THE OFFICIAL SECRETARY TO THE GOVERNOR-GENERAL

HUMAN RESOURCES

POLICY 17

PRIVACY POLICY

June 2018

CONTENTS

1. Introduction

Collection of personal information in the Office of the Official Secretary to the Governor-General (the Office) will only be done for a specified purpose and will be undertaken in strict compliance with the Australian Privacy Principles (APPs) set out in the *Privacy Act 1988* (Privacy Act) as amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012.*

2. The Privacy Act

The Privacy Act regulates how APP entities collect, hold, use and disclose personal information and how individuals can access and seek correction of that information. APP entities are:

- Commonwealth agencies, including the Office; and
- private sector organisations

which are bound by the Privacy Act.

'Personal information' is information or opinion in any form that identifies or enables identification of a person:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

The complete definition can be found at www.oaic.gov.au

2.1 Compliance with the Privacy Act

The Office is required to comply with the Privacy Act and in particular the specific APPs which regulate the collection, holding, use and disclosure of personal information.

3. Commitment

The Office is committed to ensuring the APPs pertaining to management of personal information are imbedded into policy and practices and that staff have adequate awareness of compliance requirements under the Privacy Act.

4. Purpose

This policy addresses the APP's requirement for the Office to have a clearly expressed and up to date policy about its management of personal information.

5. PERSONAL INFORMATION HANDLING PRACTICES

5.1 Collection of Personal Information

The Office collects essential personal information in order to perform its functions and activities including those contained in legislation administered by the Office. The Office only collects personal information in a limited range of categories.

These categories include:

- personal information collected from employees, job applicants, contractors and others in relation to employment or engagement through contracts;
- personal information collected by contracted service providers in compliance with contractual measures as required by the Privacy Act;
- personal information collected to assist in the administration of the Australian Honours and Awards system;
- personal information to facilitate the planning and conduct of official events, functions and visits; and
- personal information to enable processing of Freedom of Information requests, Ministerial Correspondence and Briefs.
- personal and medical information collected from employees or ceased employees in relation to compensation matters. This includes the use and disclosure of this information to an Approved Rehabilitation Provider or any other party involved in your compensation and rehabilitation.

5.2 Personal Information - privacy

The privacy of personal information is of paramount importance. All personal information will be treated in accordance with the Privacy Act and the APPs. All staff of the Office employed under the *Governor-Generals Act 1974* are subject to the Office Code of Conduct.

Any collection of personal information will only be done for the specific operational purpose of the Office and will be undertaken in strict compliance with the APPs set out in the Privacy Act

5.3 Personal Information - security

The Office is committed to ensure that all personal information is kept secure and utilised for the purpose(s) under which it was collected. The Office takes steps to protect information, including personal information, against loss, unauthorised access, use, modification or disclosure and against other misuse. These steps include password protection for accessing the Office's information systems, paper files in locked cabinets and physical and electronic access restrictions based on a "need to know basis".

Employees are also required to assess the consequences of damage from unauthorised compromise or misuse of information and apply appropriate security classifications to documents they create or handle.

Security measures, storage, standards and retention periods are consistent with those provided within the Protective Security Policy Framework issued by the Commonwealth Attorney-Generals' Department, the Australian Government Information Security Manual and the Archives Act.

6. Privacy Management Plan

To align with the *Privacy (Australian Government Agencies – Governance) APP Code 2017*, the Office will develop and implement a Privacy Management Plan. This plan will be stored in RM (F/2018/497) and will provide information on the current level of Privacy Maturity and the strategies utilised by the Office.

7. Notifiable Data Breaches Scheme

The Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act 1988 (Privacy Act) established requirements for entities in responding to data breaches. Entities have data breach notification obligations when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach. This legislation was enacted on 22 February 2018. The Office in line with this legislation is developing a data breach response plan. This plan will enable the Office to respond to a data breach, and ensure that any legal obligations are met following a data breach, in the event that one should occur for the Office.

7.1.1. Data Breach Definition

A data breach, according to the Office of the Australian Information Commissioner, is an unauthorised access or disclosure of personal information, or loss of personal information.

7.1.2. Consequences of a data breach

A data breach may cause the person involved harm to mental/physical wellbeing, financial loss or damage to their reputation. A data breach may also negatively affect the reputation of this Office, which in turn could affect (or have an adverse effect on) Office business such as the Honours process.

7.2 Data Breach Response

The Office will develop a Data Breach Response Plan. This plan will be stored in RM (F/2018/497) and will be a framework that sets out the roles and responsibilities involved in managing a data breach. It will also describe the steps that the Office will take if a data breach occurs.

8. COLLECTION AND USE OF PERSONAL INFORMATION

Any personal information collected by the Office would be collected in fulfilling the role of the entity and will be handled according to the relevant Australian Privacy Principles as detailed below.

Table 1 – Relevant Australian Privacy Principles

APP	Australian Privacy Principle text
APP 1	**Open and transparent management of personal information** 1.2 An APP entity must take such steps as are reasonable in the circumstance to implement practices, procedures and systems relating to the function of the agency. 1.3 An APP entity must have a clearly expressed and up to date policy about the management of personal information. 1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available: a. free of charge; and b. in such form as is appropriate.
APP 2	**Anonymity and pseudonymity** 2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter. 2.2 Subclause 2.1 does not apply if, in relation to that matter: a. the APP entity is required or authorised by or under an Australian law, or a court/ tribunal order, to deal with individuals who have identified themselves; or b. it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.
APP 3	**Collection of solicited personal information** 3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. 3.5 An APP entity must collect personal information only by lawful and fair means. 3.6 An APP entity must collect personal information about an individual only from the individual unless: a. the individual consents to the collection of the information from someone other than the individual. b. It is unreasonable or impracticable to do so.

APP	Australian Privacy Principle text
APP 4	**Dealing with unsolicited personal information** 4.1 If: a. an APP entity receives personal information; and b. the entity did not solicit the information; the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information. 4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1. 4.3 If: a. the APP entity determines that the entity could not have collected the personal information; and b. the information is not contained in a Commonwealth record; the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified. 4.4 If sub clause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

APP	Australian Privacy Principle text
APP 5	**Notification of the collection of personal information** 5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances: a. to notify the individual of such matters referred to in sub clause 5.2 as are reasonable in the circumstances; or b. to otherwise ensure that the individual is aware of any such matters. 5.2 The matters for the purposes of sub clause 5.1 are as follows: a. the identity and contact details of the APP entity; b. if: i. the APP entity collects the personal information from someone other than the individual; or ii. the individual may not be aware that the APP entity has collected the personal information; the fact that the entity so collects, or has collected, the information and the circumstances of that collection; c. if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order — the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection); d. the purposes for which the APP entity collects the personal information; e. the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity; f. any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity; g. that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information; h. that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint; i. whether the APP entity is likely to disclose the personal information to overseas recipients; i. if the APP entity is likely to disclose the personal information to overseas recipients — the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

APP	Australian Privacy Principle text
APP 6	**Use or disclosure of personal information** 6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless: a. the individual has consented to the use or disclosure of the information; or b. subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information. 6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if: a. the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is: i. if the information is sensitive information — directly related to the primary purpose; or ii. if the information is not sensitive information — related to the primary purpose; or b. the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or c. a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or d. the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or e. the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body. 6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if: a. the agency is not an enforcement body; and b. the information is biometric information or biometric templates; and c. the recipient of the information is an enforcement body; and d. the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph. 6.4 If: a. the APP entity is an organisation; and b. subsection 16B(2) applied in relation to the collection of the personal information by the entity; the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.
APP 10	**Quality of personal information** 10.1 An APP entity must take such steps (if any) as are reasonable in the circumstance to ensure that the personal information that the entity collects is accurate, up to date and complete. 10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purposes of the use or disclosure, accurate, up to date, complete and relevant.

APP	Australian Privacy Principle text
APP 11	**Security of personal information** 11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information: a. from misuse, interference and loss: and b. from unauthorised access, modification or disclosure 11.2 If: a. an APP entity holds personal information about an individual; and b. the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and c. the information is not contained in a Commonwealth record; and d. the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information; the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

APP	Australian Privacy Principle text
APP 12	**Access to personal information** 12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information. 12.2 Exception to access – agency: a. The APP entity is an agency; and b. The entity is required or authorised to refuse to give the individual access to the personal information by or under: i. the *Freedom of Information Act*; or ii. any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents; then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access. 12.3 Exception to access – organisation If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that: a. the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of an individual, or to public health or public safety; or b. giving access would have an unreasonable impact on the privacy of other individuals; or c. the request for access is frivolous or vexatious; or d. the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or e. giving access would be unlawful. 12.4 Dealing with requests for access the APP entity must: a. respond to the requests for access to the personal information: i. if the entity is an agency – within 30 days after the request after the request is made; or ii. if the entity is an organisation – within a reasonable period after the request is made; and b. give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

APP	Australian Privacy Principle text
APP 13	**Correction of personal information** 13.1 If: a. an APP entity holds personal information about an individual; and b. either: i. the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or ii. the individual requests the entity to correct the information: the entity must take such steps (if any) 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. 13.3 Refusal to correct information If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out: a. the reasons for the refusal except to the extent that it would be unreasonable to do so; and b. the mechanisms available to complain about the refusal; and c. any others matter prescribed by the regulations.

9. Privacy Complaints and Corrections

If there is a belief that the Office has breached the APPs or made an error with personal information, the complainant may contact the Director People and Services Branch who is the Privacy Complaint Officer for the Office. The complaint should include a brief description of the specific privacy concern, any action or dealings that has been had with a staff member to address the concerns and the complainants preferred contact details. If the complainant provides their contact details, the Director People and Services Branch will then contact them to address their concerns.

Complainants generally need to complain directly to the Office and allow 30 days for the response. If a response is not received (after 30 days), or the complainant is dissatisfied with the response, they may make a complaint to the Office of the Australian Information Commissioner (OAIC) about their privacy concerns. The OAIC can investigate privacy complaints from individuals about Australian, ACT and Norfolk Island government agencies, and private sector organisations covered by the *Privacy Act*.

Complaints to the OAIC must be made in writing. The OAIC can receive privacy complaints through the following:

- online form – OAIC Privacy Complaint Form
- email: enquiries@oaic.gov.au
- post: Office of the Australian Information Commissioner
  Office of the Australian Commissioner
  GPO Box 5218
  Sydney NSW 2001
- phone: 1300 363 992

Contact the Director People and Services Branch (Privacy Contact Officer for the Office) if you want to:

- ask questions about the Office Privacy Policy;
- query how your personal information is collected, held, used, stored or disclosed by the Office;
- obtain access to or seek correction of your personal information held by the Office; or
- make a privacy complaint about the Office.

Director People and Services Branch – Office of the Official Secretary to the Governor-General

phone: (02) 6283 3624

email: kerry.cox@gg.gov.au

post: Director People and Services Branch
Office of the Official Secretary to the Governor-General
Dunrossil Drive
Yarralumla ACT 2600

10. RELEVANT LEGISLATION AND GUIDELINES

Australian Privacy Principles 2013

Australian Privacy Principles Guidelines

Freedom of Information Act 1989

Privacy Act 1988

Privacy Amendment (Enhancing Privacy Protection) Act 2012 Commonwealth

Privacy (Australian Government Agencies – Governance) APP Code 2017

Governor-General Act 1974

Office of the Official Secretary to the Governor-General Enterprise Agreement 2015-2018

OAIC's Guide to securing personal information

Workplace Surveillance Act 2005 No 47

Workplace Privacy Act 2011

11. Review

This policy will be reviewed periodically through established consultative processes.

12th July 2018

Mark Fraser LVO OAM
Official Secretary
to the Governor-General
2018